

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing:

28 September 2000 (28.09.00)

International application No.:

PCT/JP00/01333

Applicant's or agent's file reference:

340000267971

International filing date:

06 March 2000 (06.03.00)

Priority date:

19 March 1999 (19.03.99)

Applicant:

KITAHARA, Jun et al

1. The designated Office is hereby notified of its election made:



in the demand filed with the International preliminary Examining Authority on:

24 April 2000 (24.04.00)



in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer:

J. Zahra

Telephone No.: (41-22) 338.83.38

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 340000267971	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/JP00/01333	International filing date (<i>day/month/year</i>) 06 March 2000 (06.03.00)	Priority date (<i>day/month/year</i>) 19 March 1999 (19.03.99)
International Patent Classification (IPC) or national classification and IPC G06F 12/14, 15/78, 3/06, G11B 20/10		
Applicant HITACHI, LTD.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 24 April 2000 (24.04.00)	Date of completion of this report 04 December 2000 (04.12.2000)
Name and mailing address of the IPEA/JP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP00/01333

I. Basis of the report

1. With regard to the **elements** of the international application:*

- ☒ the international application as originally filed
- ☐ the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the claims:
pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the drawings:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP 00/01333

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-12	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-12	NO
Industrial applicability (IA)	Claims	1-12	YES
	Claims		NO

2. Citations and explanations

Claim 1

Document 1 (JP, 05-053921, A) cited in the international search report discloses an information processing device which is provided with both a CPU (61) as the main circuit (11) and an encrypting/decrypting circuit (12) within integrated circuit (1) and which carries out the encryption of information within a semiconductor chip containing a control device.

The invention disclosed in Claim 1 does not involve an inventive step in the light of this existing prior art.

Moreover, Document 2 (JP, 64-041947, A) cited in the international search report discloses an information processing device provided with a CPU (2), an encryption device (9) and a decryption device (10) within a single chip microcomputer and which carries out the encryption of information within a semiconductor chip containing a control device.

The invention disclosed in Claim 1 does not involve an inventive step in the light of this existing prior art.

Document 5 (newly cited) (JP, 10-275115, A (Nippon telegraph and Telephone Corp.), October 13, 1998 (13.10.98), especially paragraph 0023; (Family: none))

discloses an information processing device wherein a control section (33), an encryption processing part (34) and an encryption/decryption key storage part (35) are provided on the inside of a computer card (13) for carrying out the encryption of plain text data using an encryption key in a process in which plain text data evolved in the storage device of an information terminal device (11) is transferred to the external storage device (12).

Paragraph 0023 of said document also discloses the feature of accomodating the encryption algorithm storage means, the key storage means, the encryption processing means and the decryption processing means which constitute a computer card within a single-chip element.

The invention disclosed in Claim 1 does not involve an inventive step in the light of this existing prior art.

Claim 2

The feature of the inventions disclosed in Documents 1, 2 and 5, wherein the data to be encrypted is not allowed to leave the semiconductor chip without having been encrypted, is a matter which can be determined by a person skilled in the art as necessary and, therefore, this claim does not involve an inventive step.

Claim 3

The feature of the inventions disclosed in Documents 1, 2 and 5, wherein the data to be encrypted is not allowed to leave the semiconductor chip without having been encrypted is a matter which can be determined by a person skilled in the art as necessary and, therefore, this claim does not involve an inventive step.

Claim 4

Document 1 indicates that the CPU (61) is a single chip

microcomputer.

The feature of storing encrypted information in the storage device contained in the single chip microcomputer disclosed in Documents 1 and 2 is a matter which can be applied by a person skilled in the art and, therefore, this claim does not involve an inventive step.

Claim 5

The feature of decrypting encrypted data when processing information in the inventions disclosed in Documents 1, 2 and 5 is an obvious process for a person skilled in the art and, therefore, this claim does not involve an inventive step.

Claim 6

A person skilled in the art would easily conceive of connecting the inventions disclosed in Documents 1, 2 and 5 to a known network and, therefore, this claim does not involve an inventive step.

Claim 7

Since providing a plurality of processing devices and allowing each device to carry out a separate process is common practice, the feature of applying the inventions disclosed in Documents 1, 2 and 5 to such a structure does not involve an inventive step.

Claim 8

The feature of limiting the encrypted data to be processed to programmes as disclosed in Documents 1, 2 and 5 does not involve an inventive step.

Claim 9

Since the inventions in Documents 1 and 2 both have a microprocessor and a device for carrying out encryption

processing according to an encryption algorithm, the invention disclosed in Claim 9 does not involve an inventive step.

Claim 10

Document 3 (JP, 04-163768, A) cited in the international search report discloses the feature wherein the data stored in a file storage section on a disc storage medium undergoes data conversion by means of a data conversion key (encryption) and the feature wherein file management information is encrypted and stored in the management storage section on a disc storage medium. Since it would be easy for a person skilled in the art to conceive of carrying out the decryption process as in this known technique, using the inventions disclosed in Documents 1 and 2, the invention disclosed in Claim 10 does not involve an inventive step.

Moreover, Document 4 (JP, 09-044407, A) cited in the international search report discloses the feature of preventing the contents of a file leaking by encrypting the record pointer that is the file arrangement information. Since it would be easy for a person skilled in the art to conceive of carrying out the decryption process of the file arrangement information as in this known technique, using the inventions disclosed in Documents 1, 2 and 5, the invention disclosed in Claim 10 does not involve an inventive step.

Claims 11 and 12

Both the features of connecting a disc controller to a plurality of magnetic disc devices and of connecting the disc controller to an information processing device are commonly known and, therefore, these claims do not involve an inventive step.

P C T

REC'D 15 DEC 2000

WIPO


PCT

国際予備審査報告

(法第12条、法施行規則第56条)
[PCT36条及びPCT規則70]

出願人又は代理人 の書類記号 340000267971	今後の手続きについては、国際予備審査報告の送付通知(様式PCT/ IPEA/416)を参照すること。	
国際出願番号 PCT/JPO0/01333	国際出願日 (日.月.年) 06.03.00	優先日 (日.月.年) 19.03.99
国際特許分類 (IPC) Int. Cl ⁷ G06F12/14, G06F15/78, G06F3/06, G11B20/10		
出願人 (氏名又は名称) 株式会社日立製作所		

1. 国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条 (PCT36条) の規定に従い送付する。
2. この国際予備審査報告は、この表紙を含めて全部で 4 ページからなる。
- ☐ この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び/又はこの国際予備審査機関に対してした訂正を含む明細書、請求の範囲及び/又は図面も添付されている。
(PCT規則70.16及びPCT実施細則第607号参照)
この附属書類は、全部で ページである。
3. この国際予備審査報告は、次の内容を含む。
- I ☒ 国際予備審査報告の基礎
- II ☐ 優先権
- III ☐ 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
- IV ☐ 発明の単一性の欠如
- V ☒ PCT35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
- VI ☐ ある種の引用文献
- VII ☐ 国際出願の不備
- VIII ☐ 国際出願に対する意見

国際予備審査の請求書を受理した日 24.04.00	国際予備審査報告を作成した日 04.12.00	
名称及びあて先 日本国特許庁 (IPEA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 梅 村 勁 樹 	5 N 7 3 1 3
電話番号 03-3581-1101 内線 3545		

I. 国際予備審査報告の基礎

1. この国際予備審査報告は下記の出願書類に基づいて作成された。(法第6条(PCT14条)の規定に基づく命令に
応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。
PCT規則70.16, 70.17)

☒ 出願時の国際出願書類

- ☐ 明細書 第 _____ ページ、 出願時に提出されたもの
明細書 第 _____ ページ、 国際予備審査の請求書と共に提出されたもの
明細書 第 _____ ページ、 _____ 付の書簡と共に提出されたもの
- ☐ 請求の範囲 第 _____ 項、 出願時に提出されたもの
請求の範囲 第 _____ 項、 PCT19条の規定に基づき補正されたもの
請求の範囲 第 _____ 項、 国際予備審査の請求書と共に提出されたもの
請求の範囲 第 _____ 項、 _____ 付の書簡と共に提出されたもの
- ☐ 図面 第 _____ ページ/図、 出願時に提出されたもの
図面 第 _____ ページ/図、 国際予備審査の請求書と共に提出されたもの
図面 第 _____ ページ/図、 _____ 付の書簡と共に提出されたもの
- ☐ 明細書の配列表の部分 第 _____ ページ、 出願時に提出されたもの
明細書の配列表の部分 第 _____ ページ、 国際予備審査の請求書と共に提出されたもの
明細書の配列表の部分 第 _____ ページ、 _____ 付の書簡と共に提出されたもの

2. 上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である _____ 語である。

- ☐ 国際調査のために提出されたPCT規則23.1(b)にいう翻訳文の言語
☐ PCT規則48.3(b)にいう国際公開の言語
☐ 国際予備審査のために提出されたPCT規則55.2または55.3にいう翻訳文の言語

3. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

- ☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際予備審査(または調査)機関に提出された書面による配列表
☐ 出願後に、この国際予備審査(または調査)機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

4. 補正により、下記の書類が削除された。

- ☐ 明細書 第 _____ ページ
☐ 請求の範囲 第 _____ 項
☐ 図面 図面の第 _____ ページ/図

5. ☐ この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。(PCT規則70.2(c) この補正を含む差し替え用紙は上記1.における判断の際に考慮しなければならず、本報告に添付する。)

V. 新規性、進歩性又は産業上の利用可能性についての法第12条(PCT35条(2))に定める見解、それを裏付ける文献及び説明

1. 見解

新規性(N)	請求の範囲	1-12	有
	請求の範囲		無
進歩性(IS)	請求の範囲		有
	請求の範囲	1-12	無
産業上の利用可能性(IA)	請求の範囲	1-12	有
	請求の範囲		無

2. 文献及び説明(PCT規則70.7)

請求の範囲1

国際調査報告書に引用された文献1(JP, 05-053921, A)には、集積回路1内に、主回路11としてのCPU61と、暗号化・解読回路12を設け、情報の暗号化を制御装置を含む半導体チップ内で実行する情報処理装置が、記載されている。

かかる公知技術の存在により、請求項1に記載された発明は進歩性を有しない。

また、国際調査報告書に引用された文献2(JP, 64-041947, A)には、シングルチップ・マイクロコンピュータ内に、CPU2と、暗号化器9と、復号化器10とを設け、情報の暗号化を制御装置を含む半導体チップ内で実行する情報処理装置が、記載されている。

かかる公知技術の存在により、請求項1に記載された発明は進歩性を有しない。

文献5(追加): JP, 10-275115, A(日本電信電話株式会社)13. 10月. 1998(13. 10. 98), 特に段落0023, ファミリーなし
には、情報端末装置11の記憶装置に展開された平文データを外部記憶装置12へ転送する過程で、暗号化鍵を用いて平文データに暗号化処理を施すための、制御部33、暗号処理部34及び暗号化・復号鍵蓄積部35を計算機カード13の内部に設けてなる情報処理装置が、記載されている。

かかる文献の段落0023には、計算機カードを構成する暗号化アルゴリズム記憶手段、鍵蓄積手段、暗号化処理手段及び復号処理手段をワンチップ素子により機能構成することも、記載されている。

かかる公知手段の存在により、請求項1に記載された発明は進歩性を有しない。

請求の範囲2

文献1, 2, 5記載の技術において、暗号化すべきデータを暗号化しないまま半導体チップの外へ出さないようにすることは、当業者が所望により適宜決定できることであるから、この点に進歩性を認めることはできない。

請求の範囲3

文献1, 2, 5記載の技術において、暗号化しなくてもよいデータを暗号化しないまま半導体チップの外へ出すようにすることは、当業者が所望により適宜決定できることであるから、この点に進歩性を認めることはできない。

補充欄 (いずれかの欄の大きさが足りない場合に使用すること)

第 V 欄の続き

請求の範囲 4

文献 1 において、CPU 61 はシングルチップ・マイクロコンピュータであると記載されている。

文献 1, 2 に記載されるシングルチップ・マイクロコンピュータが有する記憶装置に、暗号化された情報を格納することは、当業者の適宜採用し得る事項であり、この点に進歩性を認めることはできない。

請求の範囲 5

文献 1, 2, 5 記載の技術において、情報の処理に際し暗号化されたデータを復号化することは、当業者にとって自明の処理であって、この点に進歩性を認めることはできない。

請求の範囲 6

文献 1, 2, 5 記載の技術を周知のネットワークに接続することは、当業者が容易に想到し得ることであり、この点に進歩性を認めることはできない。

請求の範囲 7

処理装置を複数個設け、それぞれの処理装置でそれぞれの処理を行うことは周知慣用であるから、文献 1, 2, 5 記載のものを、そのような構成に適用した点に進歩性を認めることはできない。

請求の範囲 8

文献 1, 2, 5 記載の技術において、処理すべき暗号化されたデータが、プログラムであると限定した点に、進歩性を認めることはできない。

請求の範囲 9

文献 1, 2 記載のものも、それぞれマイクロプロセッサと、暗号化アルゴリズムに従って暗号化処理を実行する装置を有しているから、請求の範囲 9 記載の発明は、進歩性を有していない。

文献 5 記載の制御部 33 は、CPU を具備するものであることが、段落 0031 に記載されているから、請求の範囲 9 記載の発明は進歩性を有しない。

請求の範囲 10

国際調査報告書に引用された文献 3 (JP, 04-163768, A) には、ディスク記憶媒体上のファイル記憶部に記憶させるデータを、データ変換鍵によりデータ変換すること (暗号化)、およびファイル管理情報を暗号化してディスク記憶媒体上の管理記憶部に記録することが、記載されている。かかる公知技術における復号処理を、文献 1, 2 記載の技術により行うことは当業者が容易に想到し得たものであるから、請求の範囲 10 記載の発明は進歩性を有しない。

また、国際調査報告書に引用された文献 4 (JP, 09-044407, A) には、ファイル配置情報であるレコードポイントを暗号化しファイル内容の漏洩防止を図る技術が、記載されている。かかる公知技術におけるファイル配置情報の復号処理を、文献 1, 2, 5 記載の技術により行うことは当業者が容易に想到し得たものであるから、請求の範囲 10 記載の発明は進歩性を有しない。

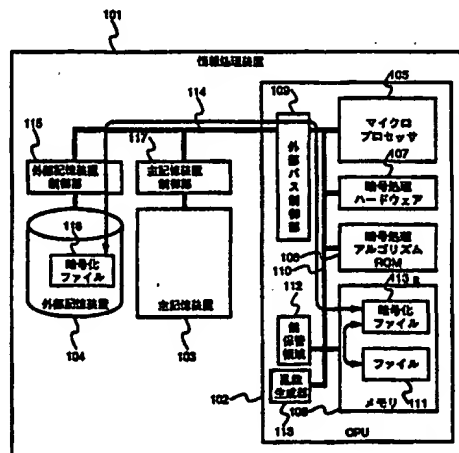
請求の範囲 11-12

ディスクコントローラを複数の磁気ディスク装置に接続すること、ディスクコントローラを情報処理装置に接続することの、いずれも周知の構成であり、この点に進歩性を認めることはできない。

(51) 国際特許分類7 G06F 12/14, 15/78, 3/06, G11B 20/10		A1	(11) 国際公開番号 WO00/57278
			(43) 国際公開日 2000年9月28日(28.09.00)
(21) 国際出願番号 PCT/JP00/01333		(81) 指定国 CN, JP, KR, SG, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)	
(22) 国際出願日 2000年3月6日(06.03.00)		添付公開書類 国際調査報告書	
(30) 優先権データ 特願平PCT/JP99/01402 1999年3月19日(19.03.99) JP			
(71) 出願人 (米国を除くすべての指定国について) 株式会社 日立製作所(HITACHI, LTD.)(JP/JP) 〒101-8010 東京都千代田区神田駿河台四丁目6番地 Tokyo, (JP)			
(72) 発明者 ; および			
(75) 発明者 / 出願人 (米国についてのみ) 北原 潤(KITAHARA, Jun)(JP/JP) 朝日 猛(ASAHI, Takeshi)(JP/JP) 大和田徹(OWADA, Toru)(JP/JP) 〒215-0013 神奈川県川崎市麻生区王禅寺1099番地 株式会社 日立製作所 システム開発研究所内 Kanagawa, (JP)			
(74) 代理人 弁理士 作田康夫(SAKUTA, Yasuo) 〒100-8220 東京都千代田区丸の内一丁目5番1号 株式会社 日立製作所内 Tokyo, (JP)			

(54)Title: INFORMATION PROCESSING DEVICE

(54)発明の名称 情報処理装置



- 101...INFORMATION PROCESSING DEVICE
- 103...MAIN STORAGE
- 104...EXTERNAL STORAGE
- 105...MICROPROCESSOR
- 106...ENCRYPTION ALGORITHM
- 107...ENCRYPTION HARDWARE
- 108...MEMORY
- 109...EXTERNAL BUS CONTROLLER
- 111...FILE
- 112...KEY STORAGE
- 113...RANDOM NUMBER GENERATOR
- 113a...ENCRYPTED FILE
- 115...EXTERNAL STORAGE CONTROLLER
- 116...ENCRYPTED FILE
- 117...MAIN STORAGE CONTROLLER

(57) Abstract

A device structure for reliably encrypting and decrypting information is provided, which is used for security with information processing device, a communication device and a file management device. Such devices comprise a plurality of semiconductor parts. Therefore, confidential data may remain in devices, for example, in a system bus and semiconductor memory for main storage. To solve this problem, a device CPU is equipped with a microprocessor, an encryption algorithm ROM, an encryption hardware, RAM, a key storage area, and an external bus control, which are all integrated into a single semiconductor chip. Encryption and decryption take place only within the CPU, and the internal operations of the CPU cannot be inferred from signals outside the CPU.

本発明は、秘密保持のために、情報を暗号化／復号化する情報処理装置や通信装置やファイル管理装置において、安全に暗号化／復号化を行う装置構成を提供するものである。

これらの装置は、複数の半導体部品から構成されている。そのため、装置内のシステムバスや主記憶を構成する半導体記憶素子に秘密にすべきデータが存在してしまう問題点がある。

そこで、本発明は以下の構成をとる。各装置のCPUに、マイクロプロセッサと、暗号処理アルゴリズムROMと、暗号処理ハードウェアと、RAMと、鍵保管領域と、外部バス制御部を設けさらに同一半導体チップ上に集積する。このCPUを内でのみ暗号化／復号化処理を行い、さらにCPU内部動作をCPU外部信号から推測不可能にする。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AG	アンティグア・バーブーダ	DZ	アルジェリア	LC	セントルシア	SD	スーダン
AL	アルバニア	EE	エストニア	LI	リヒテンシュタイン	SE	スウェーデン
AM	アルメニア	ES	スペイン	LK	スリ・ランカ	SG	シンガポール
AT	オーストリア	FI	フィンランド	LR	リベリア	SI	スロヴェニア
AU	オーストラリア	FR	フランス	LS	レソト	SK	スロヴァキア
AZ	アゼルバイジャン	GA	ガボン	LT	リトアニア	SL	シエラ・レオネ
BA	ボスニア・ヘルツェゴビナ	GB	英国	LU	ルクセンブルグ	SN	セネガル
BB	バルバドス	GD	グレナダ	LV	ラトヴィア	SZ	スワジランド
BE	ベルギー	GE	グルジア	MA	モロッコ	TD	チャード
BF	ブルキナ・ファソ	GH	ガーナ	MC	モナコ	TG	トーゴ
BG	ブルガリア	GN	ガンビア	MD	モルドヴァ	TJ	タジキスタン
BJ	ベナン	GM	ギニア	MG	マダガスカル	TM	トルクメニスタン
BR	ブラジル	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア共和国	TR	トルコ
BY	ベラルーシ	GW	ギニア・ビサオ			TT	トリニダード・トバゴ
CA	カナダ	HR	クロアチア	ML	マリ	TZ	タンザニア
CF	中央アフリカ	HU	ハンガリー	MN	モンゴル	UA	ウクライナ
CG	コンゴ	ID	インドネシア	MR	モーリタニア	UG	ウガンダ
CH	スイス	IE	アイルランド	MW	マラウイ	US	米国
CI	コートジボアール	IL	イスラエル	MX	メキシコ	UZ	ウズベキスタン
CM	カメルーン	IN	インド	MZ	モザンビーク	VN	ヴェトナム
CN	中国	IS	アイスランド	NE	ニジェール	YU	ユーゴスラヴィア
CU	キューバ	IT	イタリア	NL	オランダ	ZA	南アフリカ共和国
CY	キプロス	JP	日本	NO	ノールウェー	ZW	ジンバブエ
CZ	チェコ	KE	ケニア	NZ	ニュージーランド		
DE	ドイツ	KG	キルギスタン	PL	ポーランド		
DK	デンマーク	KP	北朝鮮	PT	ポルトガル		
		KR	韓国	RO	ルーマニア		

明 細 書

情報処理装置

5

技術分野

本発明は、情報の保管、転送時の秘密性を保つために暗号を使用する情報処理装置に関する。その中でも特に、秘密性保持の高い情報処理を構築することに関する。

10

背景技術

暗号を使用する情報処理装置の従来技術としては、以下のものがある。

ハードディスクドライブのような外部記憶装置に、情報を暗号化して記憶するものとして、特開平10-275115号公報がある。特開平10-275115号公報では、外部記憶装置12に一旦書き込まれた暗号化データY a, Y bを情報端末装置11へ転送する過程で、暗号化・復号鍵蓄積部35に蓄積された復号鍵K bを用いながら当該暗号化データY a, Y bに逐次的に復号処理を施すものである。

また、情報処理装置内に専用の暗号処理装置を設けたものとして、特開平10-214233号公報がある。特開平10-214233号公報では、携帯型PCの中にデータを暗号化して暗号化ファイルのボディ部を生成する暗号化装置を備えている。

ここで、暗号化や復号化といった暗号処理は、一般に主記憶上のデータを対象に処理するため、主記憶上に秘密にすべきデータが存在する。情報を暗号化するためには、暗号アルゴリズムに従い情報を処理しなければならないが、暗号アルゴリズムと暗号に用いる鍵情報と暗号をかける秘密情

25

報全てを、安全に処理する必要が生じる。

しかし、これらの従来技術では以下の問題が存在する。

従来技術においては、秘密情報や暗号処理の途中経過が主記憶上に存在するため、幾つかの手法で情報を取り出す事が可能になる問題がある。この問題は、CPU や主記憶などが、複数の半導体で構成されている情報処理装置において、CPU を用いて暗号処理を行うと暗号アルゴリズムや暗号をかける秘密情報や暗号処理の途中経過が主記憶上に存在するためである。

また、情報処理装置内には、情報処理装置を構成する各半導体部品を接続する信号線（例えばバス）が存在するため、この信号線を観察し、情報を解析する事により、暗号化する前のデータや復号化したデータを簡単に取り出せるという問題がある。

また、装置外部の信号線に対して暗号化したデータを送出するものとして、特開平2-297626があるが、暗号化するのに必要な鍵情報は外部から与えられており、この鍵情報の機密管理を確実に行わないと、データの暗号化が意味を成さなくなる問題がある。

発明の開示

従来技術の問題を解決するために、本発明では、以下の構成とした。

情報処理装置を構成する半導体内部で暗号化処理を施す。また、暗号化処理に必要な鍵情報も半導体内部で生成する。また、情報処理装置内の信号線上に暗号に関する情報を出力しない。情報処理装置の信号線上には、他者に観察されてもかまわない情報が出力される。この情報としては、暗号化された情報や暗号化する必要のない情報などである。なお、暗号に関する情報としては、暗号化されていない情報や暗号化された情報を復号するための情報を含む。

より具体的には、本発明の構成は、情報処理装置での処理を実行する処

理装置 (CPU) と同一半導体チップに、RAM と暗号処理アルゴリズムと暗号処理ハードウェアと、鍵情報生成ハードウェアと、鍵情報格納ハードウェアを集積したものである。なお、本発明では便宜上 CPU と読んでいるが、名称はこれに限られず、情報処理装置を構成する半導体チップであればよい。その中でも特に、情報処理装置の制御や演算処理を行う処理装置がよい。つまり、本発明は、情報処理装置を構成する 1 半導体チップ内で鍵情報の生成を含め暗号化処理が閉じているものである。さらに、本発明では、CPU が複数個あり、それぞれにおいて、暗号化処理が行う構成としてもよい。

10 また、この暗号処理が内蔵する RAM 内で処理されてもよい。

また、CPU に内蔵される RAM を主記憶として用い、アプリケーションプログラムの実行も内蔵する RAM 内で処理されるものでもよい。

また、アプリケーションプログラム自体も暗号化され、外部記憶装置には、暗号化ファイルが存在する構成にしたものでもある。

15 また、外部バスへのデータ出力を制御する外部バス制御部を設けてもよい。この外部バス制御部では、内部 RAM がアクセスされているときのデータを外部バスへ出力しないよう制御してもよい。さらに、このデータ外部バスに出力してもよい情報か否かを判断して、出力してもよい場合にデータを外部バスに出力するように制御してもよい。

20 また、通信データの暗号化／復号化を CPU 内部で処理するものである。

さらに、これらのいずれかの構成によって、情報に応じて暗号化するか否かを決定してもよい。情報が、暗号化しなくともよい情報であれば暗号化せずに情報処理装置の信号線上に出力する構成としてもよい。

さらに、本発明は、ディスクシステムコントローラ内のプロセッサ内部で暗号処理を可能にすることで、磁気ディスク上のファイル配置情報を暗号化したものも含まれる。

25

図面の簡単な説明

第1図は、本発明の情報処理装置の構成を示す図である。第2図は、本発明の情報処理装置におけるファイル生成を説明する図である。第3図は、
5 本発明の1形態である主記憶を内蔵するCPUを有する情報処理装置の構成を示す図である。第4図は、本発明の1形態である外部記憶装置に格納しているアプリケーションプログラムをCPUで暗号化する情報処理装置の構成を示す図である。第5図は、外部バス制御部の構成を示す図である。第6図は、外部バス制御部で外部バスへのデータを出力させない1実施例を
10 説明する図である。第7図は、鍵生成に必要な乱数生成部の構成を示す図である。第8図は、鍵保管部の構成を示す図である。第9図は、暗号化および復号化する装置が自分自身である場合の暗号化複合化処理と鍵の関係を
15 示す図である。第10図は、第9図の鍵の取扱いを変え、記憶しなければならない鍵情報を少なくする構成を示す図である。第11図は、暗号化する装置と復号化する装置が異なる場合の、暗号化処理と鍵の関係、複合化処理と鍵の関係を
20 示す図である。第12図は、第11図に加えて、送信者の保証情報を付加した構成を示す図である。第13図は、相手から入手する鍵情報を認証する仕組みを示す図である。第14図は、本発明をプロセッサバスおよびシステム情報処理装置に適用した場合の構成を示す図である。第15図は、本発明を通信に適用した場合の構成を示す図である。
第16図は、外部記憶装置に本発明を適用した場合を説明する図である。第17図は、第16図の構成で暗号化ファイル配置情報の書込みを説明する図である。第18図は、ディスクコントローラの構成を示す図である。
第19図は、本発明の1形態である複数のCPUを有する情報処理装置を示す
25 図である。第20図は、第19図の変形例を示す図である。第21図は、第16図に示した構成の変形例である。第22図は、第16図に示した構

成の変形例である。第23図は、第15図に示す情報処理装置がネットワークに接続されている全体システムを表わす図である。

発明を実施するための最良の形態

5 以下、図面を用いて本発明の実施例を説明する。

 まず、本発明の第一の実施例を第1図および第2図を用いて説明する。

 第1図は、少なくとも、CPU(102)、主記憶装置(103)、外部記憶装置(104)を備える情報処理装置(101)の構成を模式的に表した図である。CPU(102)、主記憶装置制御部(117)、外部記憶装置制御部(115)は、理論上のシステムバス(114)で接続され、各々に主記憶装置(103)、外部記憶装置(104)が接続
10 される。実際の信号線の接続は、第7図のようになるが、データの流を理論的に考えると、模式的に第1図のように表す事が出来る。

 CPU(102)は、マイクロプロセッサ(105)と、暗号処理アルゴリズムROM(106)と、暗号処理ハードウェア(107)と、RAM(108)と、鍵保管領域(112)と、外部バス制御部(109)からなる。さらに、これらを同一半導体チップ上に集積する。
15

 CPU(102)内部では、マイクロプロセッサバス(110)に、暗号処理アルゴリズムROM(106)と、暗号処理ハードウェア(107)と、RAM(108)と、外部バス制御部(109)が接続される。本実施例においては、CPU内部でデータに対する暗号化処理が行われる。
20

 ファイル(111)を暗号化するには、暗号処理アルゴリズムROM(106)に従い、必要であれば暗号処理ハードウェア(107)を用いて暗号化する。この時の暗号化に用いる鍵データは、CPU(102)内で生成しても良いし、あらかじめ与えられるデータを用いても良い。但し、この鍵データはCPU(102)内の鍵保管領域(112)、保持されていなければならない。暗号化処理において、途中経過のデータが生成される場合は、その途中経過のデータもRAM(108)内
25

に格納する。このようにして、ファイル(111)から暗号化ファイル(113)を生成する。

暗号化ファイル(113)は、システムバス(114)を通して外部記憶装置制御部(115)を経由して外部記憶装置(104)に格納する。

- 5 外部記憶装置(104)に格納されている暗号化ファイル(116)を復号化する場合は、逆の順序で処理を行う。

まず、外部記憶装置(104)から暗号化ファイル(116)を外部記憶装置制御部(115)を経由してRAM(108)に読み込む。次に、暗号処理アルゴリズムROM(106)に従い、必要であれば暗号処理ハードウェア(107)を用いて復号化する。

10

大量のデータを高速に暗号化／復号化するためには、暗号鍵と復号鍵が共通である共通鍵暗号系を用いる。共通鍵暗号系では、暗号と復号は処理の順序が逆になっているだけで、最小単位の処理自体は暗号化も復号化も同じである。暗号処理アルゴリズムROM(106)には、復号化処理の手順も格納しておく。また、暗号処理ハードウェア(107)は復号化でも使用する事が可能である。

15

第2図は、第1図のファイル(111)を生成するまでの過程を示したものである。

アプリケーションプログラム(201)は、稼動時以外は外部記憶装置内に格納されている。このアプリケーションプログラムに起動がかかると主記憶に展開され動作可能な状態になる。動作可能になったアプリケーションプログラム(202)は、オペレーティングシステム等への情報処理装置管理プログラムに対して、作業領域の割り当てを要求する。このとき、オペレーティングシステム等への情報処理装置管理プログラムは、作業領域(203)としてRAM(108)内の空間を割り当てる。

20

25

この状態で、アプリケーションプログラム(202)は、マイクロプロセッサ

(105)で処理され、生成された情報は作業領域(203)に格納される。この生成された情報の中から外部記憶装置に格納すべきデータをファイル(111)として生成する。

5 アプリケーションプログラム(202)自体は主記憶上に存在し、そのアプリケーションプログラムの作業領域(203)を RAM(108) 上を取るためには、オペレーティングシステム等の情報処理装置管理プログラムが管理するマイクロプロセッサが持つメモリ管理機能を用い、アプリケーションプログラムの作業領域を示す論理アドレスを RAM(108)内の物理アドレスに変換する事で可能になる。

10 鍵保持部(112)は、RAM(108)の領域内に設けられていても良いが、不揮発性でなければならない。EEPROM や FlashROM のような不揮発性の ROM で構成しても良いし、バッテリーバックアップされた SRAM で構成しても良い。バッテリーバックアップされた SRAM で構成した場合、暗号に使用した鍵を取り出そうと、情報処理装置に攻撃が加えられた場合にそれを検知し、バックアップ電源を切断する事で、鍵情報を消失させ秘密情報を守ることにも可能になる。

このように、情報の生成、暗号処理を同一半導体チップ内で行う事により、半導体チップの端子等の信号を観察するような解析方法でも、暗号のかからない秘密情報を入手する事は困難になる。

20 次に、本発明の第二の実施例を第3図を用いて説明する。

第3図は、CPU(101)内の RAM(108)を、情報処理装置(101)の主記憶として構成したものである。

この場合、外部記憶装置に格納されているアプリケーションプログラム(301)は、起動時に RAM(108)に展開され動作可能になる。動作可能になったアプリケーションプログラム(302)は、オペレーティングシステム等の情報処理装置管理プログラムに対して、作業領域の割り当てを要求する。こ

25

のとき、オペレーティングシステム等への情報処理装置管理プログラムは、作業領域(303)として RAM(108)内の空間を割り当てる。この状態で、アプリケーションプログラム(302)は、マイクロプロセッサ(105)で処理され、生成された情報は作業領域(303)に格納される。この生成された情報の中から外部記憶装置に格納すべきデータをファイル(111)として生成する。

生成されたファイル(111)は、暗号処理アルゴリズム ROM(106)に従い、必要であれば暗号処理ハードウェア(107)を用いて暗号化される。暗号化されたファイル(113)は、外部記憶装置に暗号化ファイル(116)として格納される。

第3図では、CPU 外部の主記憶装置を図示していないが、秘密情報を生成するアプリケーションプログラムとそれ以外のアプリケーションプログラムを区別し、秘密情報を生成するアプリケーションプログラムの実行は、RAM(108)で行い、それ以外のアプリケーションプログラムは、従来通り CPU 外部の主記憶装置で処理する構成を取っても良い。

このように、RAM(108)を主記憶にする事により、CPU(102)外部にはアプリケーションプログラム(301)を RAM(108)に展開する時のデータ転送しか発生せず、アプリケーションプログラム自体の処理も安全に行える。

本発明の第三の実施例を第4図を用いて説明する。

本実施例では、暗号化されたアプリケーションプログラム(401)を外部記憶装置(104)に格納している。このアプリケーションプログラムは、情報処理装置の CPU 内で復号化される。このため、バス(114)上には、復号化されたアプリケーションプログラムは出力されず、復号化されたアプリケーションプログラムは CPU 内部で閉じている。このため、他者がこのアプリケーションプログラムを観察することを防止できる。

以下、第三の実施例の詳細を説明する。外部記憶装置内の暗号化アプリケーションプログラム(401)は、起動時にバス(114)を通して情報処理装置

内の RAM(108)に転送される。転送された暗号化アプリケーションプログラム(402)は、RAM(108)に展開される。展開された暗号化アプリケーションプログラム(402)は、RAM(108)内で復号化され、アプリケーションプログラム(403)になる。この状態でアプリケーションプログラム(403)が動作し、
5 RAM(108)内の作業領域(404)を用いながら情報を生成する。生成された情報は必要な部分が選択され、ファイル(111)としてまとめられる。ファイル(111)を暗号化し、暗号ファイル(113)を生成する。暗号ファイル(113)を暗号ファイル(116)として外部記憶装置(104)に格納する。

このように、アプリケーションプログラム自体も暗号化ファイルの一つとして外部記憶装置に格納する事により、さらに安全性を高める事も出来る。
10

なお、この暗号化アプリケーションプログラム(401)を生成するためには、アプリケーションプログラム自体をファイル(111)として、暗号化を行うものである。

15 次に、第5図および第6図を用いて、本発明の外部バス制御部の説明をする。

第一から第三の各実施例に用いられる外部バス制御部(109)は、CPU内部と外部とのデータの入出力を制御するものである。例えば、マイクロプロセッサ(105)が行う、暗号処理のために暗号処理アルゴリズムROM(106)又は、暗号処理ハードウェア(107)又は、RAM(108)へのアクセスをCPU(102)外部に出ないように制御する。但し、マイクロプロセッサ(105)のアクセスがCPU外部に出力されても構わないものであれば、外部に出力されるよう制御してもよい。この場合、CPU外部に出力されても構わないデータとしては、暗号処理を行わず他の情報処理装置に転送するデータなどがある。
20

25 外部バス制御部(501)は、マイクロプロセッサ(502)の制御バス(503)、アドレスバス(504)、データバス(505)と、CPUの外部へ出る外部制御バス

(506)、外部アドレスバス(507)、外部データバス(508)の間にあり、外部制御バス生成部(509)と、アドレス比較部(510)と、アドレス方向制御部(512)と、データ方向制御部(513)と、マスク信号生成部(511)と、信号マスク部(514)(519)から構成される。

5 制御バス(503)と外部制御バス(506)は、マイクロプロセッサからのバスサイクル開始信号、バス方向指示信号、バスサイクル終了信号、バス調停信号等が通される。これらの信号によりバスサイクルが制御される。

10 外部制御バス生成部(509)は、マイクロプロセッサからのバスサイクル開始信号、バス方向指示信号、バスサイクル終了信号、バス調停信号等を監視する。外部制御バス生成部(509)は、マイクロプロセッサがバスアクセス権を所有しているか否かを判断し、その情報をアドレス方向制御部(512)に伝える。また、同じ情報をアドレス比較器(510)にも伝える。アドレス比較器(510)は、CPU(102)内部の暗号処理アルゴリズム ROM(106)、暗号処理ハードウェア(107)、RAM(108)が割り当てられているアドレスを把握しており、アドレスバス(504)又は、外部アドレスバス(507)から入力されるアドレスと比較する。

15 外部制御バス生成部(509)が制御バス(503)からマイクロプロセッサがバスアクセス権を所有していると判断すると、アドレス比較器(510)はマイクロプロセッサからのアドレスを監視し、RAM(108)のアドレスへのアクセスと検出すると、外部制御バス生成部(509)に伝え、外部バス制御信号を駆動させない。また、マスク信号生成部(511)にも伝え、信号マスク部(514)(519)にマスク信号を出力し、外部アドレスバス(507)、外部データバス(508)を駆動しないように制御する。もしくは、強制的にアドレスの値やデータの値を固定してしまう。

25 外部制御バス生成部(509)が制御バス(503)からマイクロプロセッサがバスアクセス権を所有していないと判断すると、アドレス比較器(510)は外部

アドレスバスを監視し、RAM(108)のアドレスへのアクセスと検出すると、外部制御バス生成部(509)に伝える。外部制御バス生成部(509)は、制御バス(503)へこのバスサイクルを伝達しない。もしくは、信号マスク部(514)(519)にマスク信号を出力し、アドレスバス(504)、データバス(505)を駆動しないように制御する。または、強制的にアドレスの値やデータの値を固定してしまう。

アドレスの値やデータの値を固定する方法として、第6図のように、信号マスク部(601)のゲート(602)と信号マスク部(603)のゲート(604)のように、ゲートの論理を変える事により実現できる。

10 このように、アドレス信号マスク回路で、RAM(108)領域以外の読み書きされても問題ない領域にアドレスを変換する事も可能である。

これにより、CPU(102)内部の処理をCPU(102)のバスであるシステムバス(114)を観察する事で推測する事が不可能になる。よって、CPU(102)内部で行う暗号処理の安全性が高まる。

15 次に第7図から第13図を用いて、鍵情報の取り扱いについて説明する。

暗号化、複合化には鍵情報が必要であり、この鍵情報の秘匿化がシステム全体の安全性を高める。従来は、鍵情報を外部から与え、その鍵を人間が厳重に管理することで、システムの安全性を高めてきた。

20 本発明では、半導体内部で暗号化に必要な鍵情報を生成し、その情報は、半導体内部にのみ保持し、半導体外部に出力する場合は特定の相手にのみ分かる手段で出力することを特徴とする。鍵情報は乱数を用いて生成する。論理的に乱数を生成する場合、一般に疑似乱数として生成する。これは、ある種情報から複数の演算をくり返すことにより、離散した数値列を求めるものである。ところが、この疑似乱数は、種情報が同じであれば、同じ
25 順序で離散した数列を生成してしまうため、種情報を入手すれば、同じ乱数を生成でき、再生可能乱数になってしまう。よって、種情報を厳重に

管理する必要性が生じる。そこで本発明では、種情報を必要としない乱数生成器(113)を設ける。

第7図は物理現象を用いて乱数を生成する乱数生成器(113)の構成例を示している。第7図では、乱数生成器(113)は、定電圧ダイオードやツェナーダイオードのノイズを元に乱数を生成する。第7図は、定電圧ダイオード(701)、抵抗(702)とコンデンサ(703)で構成されるローパスフィルタ(704)、コンパレータ(705)、フリップフロップ(706)で構成される。

定電圧ダイオード(701)は、信号波形(707)のようにノイズを発生する。このノイズは、定電圧ダイオード(701)の内部の半導体接合部分で生じる雪崩降伏がランダムに起きることに起因する物理現象である。このノイズをローパスフィルタ(704)を通すと信号波形(708)のように信号波形(707)の平均値に近い値をとる。この2つの信号をコンパレータ(705)に入力することにより、信号波形(709)のような、ランダムなパルス幅をもつ2値信号に変換することが出来る。この信号をさらにフリップフロップ(706)で半導体素子内の基準クロックに同期化させ、ランダムビット信号波形(710)を得る。

このランダムなビット列を必要なビットだけ、シフトレジスタに入力するなり、単位時間のパルスの数を計測するなりして乱数を得る。

これにより、乱数生成に種がいらず、再生不可能な乱数を得ることが出来る。また、ローパスフィルタ(704)により、ノイズを含む信号(707)の平均値(708)を求め、その平均値とノイズを含む信号を比較することにより、定電圧ダイオードの電圧に温度等による電圧変動等が生じて、乱数生成に影響が及ばない乱数生成器を構成することが出来る。

第7図では、定電圧ダイオードをノイズ源として用いているが、物理現象に基づくノイズを発生する物であれば、これに限る物ではない。

第8図は、生成した鍵情報など秘密にしておく情報を格納する鍵保管領域の構成例を示している。第8図は、鍵保管領域(112)を、バッテリバック

アップされた SRAM で構成した例を示したものである。

本発明の CPU(102)を、SRAM(804)と SRAM 制御回路(809)、その他の CPU 内部論理ブロック(802)に分け、SRAM(804)と SRAM 制御回路(809)専用の電源(805)と、内部論理ブロック(802)用の主電源(803)をそれぞれ設ける。主電源(803)と鍵保管領域(112)用電源(805)は、タイオード(806)(807)を介して SRAM(804)の電源(808)として供給される。また、同じ電源(808)は SRAM 制御回路(809)の電源としても使用する。ゲート(810)は、内部論理ブロックで使用されている初期化信号(811)と主電源(803)とを監視し、主電源(803)へ電力が供給されておりなおかつ内部論理ブロックの初期化が終了するまで、SRAM(804)への信号を全て無効になるように固定する。これにより、鍵保管領域(112)にのみ電力を供給し、他の部分への電力供給を停止した状態でも、余分な漏れ電流等を無くすることができ、さらに電力供給を停止した部分に、ノイズ等が印加されたり、動作保証以下の電圧で誤動作したとしても、その影響を遮断することができる。ゲート(810)が“L”を出力すると、ゲート(812)は“L”を出力し、アドレス信号線(813)の電圧が何であっても変化しない。また、ゲート(815)も“L”を出力しバッファ(816)の出力インピーダンスを高くするため、データ信号線(814)へ漏れ電流を流すことがなくなる。また、ゲート(820)も“L”を出力するため、バッファ(821)の出力インピーダンスを高くするため、データ信線(823)の電圧が何であっても、データ信号線(819)へ伝えることがない。また、ゲート(824)は“H”を出力し制御信号(826)を無効化して、SRAM の動作を止める。さらに、ゲート(810)(812)(815)(820)(824)、バッファ(821)を CMOS 構造の素子で構成にすることにより、入力信号(814)(817)(823)(822)(825)に流れる漏れ電流を微小に押さえることができるため、内部論理ブロック(802)への電力供給が停止しても、鍵保管用電源(805)の電力が漏れ出ることはない。これにより、鍵保管用電源(805)から消費する電力を必要最小限に抑えることができ、

バックアップバッテリー (828) の寿命を長くすることができる。

主電源 (803) から電力が供給され、内部論理ブロック (802) の初期化が終了すると、ゲート (810) は "H" を出力する。すると、ゲート (812) は、アドレス信号線 (813) のデータをアドレス信号線 (814) に伝える。ゲート (815) は、
5 SRAM 読み出し信号 (817) が有効なときにバッファ (816) を有効にしデータ信号線 (819) のデータをデータ信号線 (818) に伝える。ゲート (820) は、SRAM 書き込み信号 (822) が有効なときにバッファ (821) を有効にしデータ信号線 (823) のデータをデータ信号線 (819) に伝える。ゲート (824) は、制御信号線 (825) のデータを制御信号線 (826) へ伝える。これにより、正常に
10 SRAM (804) をアクセス可能になる。

また、CPU (102) を収納する筐体等のケースに各種感知器を設け、それらからの信号を元に、バッテリー (828) から供給される鍵保管用電源 (805) を制御する異常検出器 (827) を設ける。筐体等のケースの分解、解体等の異常を検出したときに、SRAM (804) への電力供給を停止し、鍵情報を消失させてしまうものである。さらには、主電源 (803) から電力が供給されている場合には、異常検出器 (827) が作動して、鍵保管用電源 (805) からの電力供給を
15 絶っても、主電源 (803) から SRAM (804) へ電力が供給されてしまうため、異常検出信号 (829) を内部論理ブロック (802) に入力し、異常を伝え、動作を制限または停止させる。

20 CPU (102) 内で、SRAM (804) への電源を統合してもよいが、主電源とバッテリーからの電力を、異常検出器 (827) 内で統合し、いかなる場合でも異常を検出したら、SRAM (804) へ電力が供給を絶つ構成にしてもよい。

異常検出器 (827) と CPU (102) を接続する信号線および電源線は極力短くかつ基板の内部を通す等、簡単には探針不可能なように実装する必要がある。
25 さらに、配線箇所の異なる、複数の信号線で接続する等、防御手段を講じる必要がある。これにより、装置を分解されても秘密鍵が半導体素子

外部に漏れることがなくなる。

本発明で生成する鍵は、半導体自体を識別する為に必要な鍵と、情報を暗号化するのに用いる鍵の２種類あり、それぞれ使用目的が異なる。前者を認証用の鍵、後者を情報暗号化の為に鍵とする。頻繁に鍵を生成する必要がある鍵は、情報暗号化の為に鍵であり、基本的には情報暗号化の度に生成する。認証用の鍵は、月単位や年単位といった定められた期間毎に生成し、半導体自体を識別する情報として用いる。

第９図は、暗号化した装置と復号化する装置が同一である場合の、暗号化鍵と復号化鍵の取り扱いを示したものである。

半導体である CPU(102) 内部で生成した情報(901)を暗号化し、外部記憶装置(104)等に暗号化ファイル(116)として格納し、再び CPU(102)内部で使用するために復号化する場合、鍵情報(902)は CPU(102)内部にのみ存在すれば良い。暗号化ファイル(113)(116)をこの CPU(102)でのみ扱えるようにするためには、鍵情報(902)を CPU(102)内部の乱数生成器(113)で生成し、鍵保管領域(112)にのみ保管しておく。

また、複数の情報(903)、(905)に対して暗号化する場合に、それぞれ異なる暗号鍵(904)、(906)を用いる場合は、それぞれの鍵情報(904)、(906)を鍵保管領域(112)に保管する必要がある。

図では、メモリ(108)内で暗号化処理と復号化処理を行う構成を図示しているが、CPU(102)内の処理であれば、暗号アルゴリズム(106)を用いた方法でも、暗号処理ハードウェア(107)を用いた方法でも良い。

また、第１０図に示したように、鍵保管領域(112)内には、予め乱数生成器(113)で生成した鍵(1001)のみを保管し、情報(1002)(1003)を暗号化する度に、それぞれの情報に対応して生成した鍵(1004)(1005)を鍵(1001)で暗号化し、暗号化鍵(1006)(1007)を作る。情報(1002)(1003)は、それぞれ鍵(1004)(1005)を用いて暗号化し、暗号化ファイル(1008)(1009)を生成する。

このようにして、生成した暗号化ファイル(1008)と暗号化鍵(1006)とをまとめてファイル(1010)として外部記憶装置格納し、生成した暗号化ファイル(1009)と暗号化鍵(1007)とまとめてファイル(1011)として外部記憶装置格納することで、鍵保管領域(112)に格納する鍵情報を削減しても良い。

- 5 第11図は、情報を暗号化する装置と暗号化された情報を復号化する装置が異なる場合の鍵の取り扱いを示したものである。この場合、相手が正しいか否か確認する事が必要になる。これを、相手を認証すると呼ぶ。

- 10 相手を認証する手段としては、非対象鍵暗号を用いて行う。非対象鍵とは、情報を暗号化し暗号文にする鍵と暗号文を復号化し情報に戻す鍵が異なる暗号をさす。非対称鍵暗号は公開鍵暗号とも呼ばれ、暗号化鍵と復号化鍵の2つの鍵のうち片方を公開し、もう一方は秘密にして用いる。暗号化鍵で暗号化した情報は、対応する復号化鍵のみで復号化が可能である。つまり、二つの鍵のうち、公開する方を公開鍵、秘密にする方を秘密鍵とすると、公開鍵で暗号化した暗号文は、秘密鍵でのみ復号可能であり、秘密鍵で暗号化した暗号文は、公開鍵でのみ復号可能である性質を持つ。これを
15 用いることにより。特定の相手にのみ解る手段で情報を送る事や、発信者を特定する事が可能になる。

- 20 特定の相手にのみ情報を送りたい場合は、相手の公開鍵を入手し、相手の公開鍵を用いて送りたい情報を暗号化する。このようにして出来た暗号文は、同じ公開鍵では復号化できず、相手が秘密にしている秘密鍵でのみ復号化が可能な暗号文となる。これにより、特定の相手にのみに情報を伝達する事が可能になる。一般には、非対称暗号(公開鍵暗号)は処理が複雑で、時間も必要とする事から実際の情報の暗号は、対称鍵暗号(共通鍵暗号)で暗号化し、この暗号化で使用する鍵を毎回乱数より生成し、この鍵情報を
25 を非対称鍵暗号(公開鍵暗号)を用いて、相手に秘密裏に送る方法をとる。

送信者を特定する方法は、情報を送る側が情報そのものまたは、情報に

対応する情報(ダイジェスト等)を秘密鍵で暗号化した暗号化情報を相手に送る。相手は、送信側の公開鍵を入手し、送られてきた暗号化情報を送信側の公開鍵で復号化し、正当な内容と判断することで、送信側のみが所有する秘密鍵で暗号化されていたと判断し、送信側が正当であると判断出来る。

第11図において、装置A(1101a)および装置B(1101b)では、予め各々の装置自身が装置識別情報として、公開鍵(1104a)(1104b)と秘密鍵(1105a)(1105b)を生成しておく。これらの鍵は、剰余演算を用いた公開鍵暗号では、二つの素数積を用いて生成される。素数は乱数生成(1102a)(1102b)し、その乱数が素数であるか否かを判断し生成する(1103a)(1103b)。ここで生成した鍵は、半導体自体を識別する為に必要な鍵である。

ここで、情報(1116)を装置A(1101a)から装置B(1101b)へ送る事を考える。

装置A(1101a)から装置B(1101b)にのみ解釈出来る手段で、情報(1116)を送るためには、情報(1116)を暗号化して送る事になるが、その時に使用する鍵は、その時のみ有効で、他の情報転送時には他の鍵を使用した方が、万が一鍵情報が漏洩しても被害を最小限に食い止める事ができる。その為には、毎回生成する情報(1116)を暗号化する共通鍵(1111)を、装置Bにのみ伝えなければならない。

これを実現するためには、まず装置A(1101a)は、装置Bを(1101b)へ公開鍵転送要求(1106)を出す。これをうけて、装置Bを(1101b)は装置B公開鍵(1104b)を装置A(1101a)へ転送する(1107)。装置A(1101a)は、乱数を生成し(1109)、その乱数を元に共通鍵(1111)を生成する(1110)。生成した共通鍵(1111)を、装置B(1101b)から受け取った、装置B公開鍵(1108)を公開鍵暗号化し(1112)、暗号化鍵情報(1113)を生成する。また、共通鍵(1111)

で情報(1116)を共通鍵暗号化(1115)し、暗号化情報(1117)を生成する。この暗号化鍵情報(1113)と暗号化情報(1117)を送ることにより、装置 B にのみ解釈可能な状態で、情報(1116)を送る事ができる。装置 B(1101b)では、受け取った暗号化鍵情報(1119)を装置 B 秘密鍵(1105b)で公開鍵復号化し(1120)、共通鍵(1121)を取り出し、この共通鍵(1121)で受け取った暗号化情報(1122)を共通鍵復号化し(1123)、情報(1124)を得る。

さらに、情報転送(1118)が装置 A(1101a)から送られた事を証明するためには、第 1 2 図のように、情報(1116)のダイジェストをハッシュ関数(1201)を用いて、ハッシュ値(1102)として求め、このハッシュ値(1102)を、装置 A 秘密鍵(1105a)で公開鍵暗号化し(1203)、暗号化ハッシュ値(1204)を生成する。装置 A 公開鍵(1104a)を装置 B(1101b)へ転送し(1205)、暗号化ハッシュ値(1204)を装置 A(1101a)の署名として転送する(1206)。装置 B(1101b)では、受け取った装置 A 公開鍵(1207)を用いて、暗号化ハッシュ値(1208)を公開鍵復号化し(1209)、装置 A(1101a)で生成したハッシュ値(1210)を得る。一方、受け取った情報(1124)から、ハッシュ関数(1211)を用いて、ハッシュ値(1212)を求める。この二つのハッシュ値(1210)(1212)を比較し(1213)、結果が同じであれば、情報(1124)の送り主を装置 A(1101a)と確認する事ができる。

第 1 2 図では、情報(1116)のハッシュ値を求める方法を示したが、情報(1116)のデータの大きさが小さい場合、情報そのものを装置 A 秘密鍵(1105a)で暗号化し、装置 A 公開鍵(1104a)と共に転送しても良い。

相手の公開鍵を入手する方法は、図に示したように、相手から入手しても良いし、相手と利害関係のない第三者から入手仕手も良い。

ここで、相手から公開鍵を入手する場合に、入手した公開鍵が本当に正しいか、他人が相手に成り済ましていないかを確認する必要が生ずる。

第 1 3 図は、第 1 1、1 2 図において相手から受け取った公開鍵が本当

に正しいか否かを確認する手段を示したものである。第13図は、各装置を認証する認証局として、装置C(1301)を設けた構成をとったものである。装置C(1301)は、システムに参加する各装置の公開鍵を認証する。そのために、装置C(1301)内部で乱数生成し(1302)、その乱数から素数を生成し(1303)、装置Cの公開鍵(1304)と秘密鍵(1305)を生成しておく。この装置Cの秘密鍵がシステム内で最も機密にしなければならない情報になる。

装置A(1101a)、装置B(1101b)で、装置識別用に生成した公開鍵(1104a)(1104b)と秘密鍵(1105a)(1105b)の内、それぞれの公開鍵を装置C(1301)に対して、認証依頼として転送する(1316a)(1316b)。認証依頼を受けた装置C(1301)は、受け取った各装置の公開鍵(1306a)(1306b)を、装置Cの秘密鍵(1305)で公開鍵暗号化し(1307a)(1307b)、認証書(1308a)(1308b)を生成する。この認証書と装置Cの公開鍵(1304)を一緒にした認証結果(1309a)をそれぞれの装置へ転送する(1317a)(1317b)。

各装置は、自分の公開鍵の認証書を記憶しておく。情報転送の為の公開鍵要求がきたら、自分の公開鍵(1105b)を転送すると共に、認証書も転送し、自分装置Cによって、認証されている事を示す。受け取った認証書(1312)は、記憶してある装置Cの公開鍵を用いて、公開鍵復号化される(1313)。認証書(1312)内の装置Bの公開鍵(1314)を取り出し、装置B(1101b)から転送された公開鍵(1108)と比較する(1315)ことにより、装置Bの公開鍵の正当性を検証する。

装置Cによる認証作業における装置とその公開鍵の対応は、電子的な確認だけでなく、装置に改良等第三者の手が加えられていないか等、細かい検査ののちに行われるものである。

このような、手順を踏むことにより相手から、公開鍵を入手しても正当性を確認する事が可能になる。

次に、本発明の第四の実施例を、第14図を用いて説明する。

第14図は、一般的な情報処理装置の構成を模式的に表した図である。

5 情報処理装置(1401)は、複数の半導体部品から構成されている。CPU(1402)はプロセッサバス(1404)で、キャッシュメモリと主記憶制御部(1405)に接続される。主記憶制御部(1405)は、システムバス制御部を含み、メモリバス(1413)とシステムバス(1407)が接続される。メモリバス(1413)には、主記憶装置(1406)が接続され、システムバス(1407)には、外部記憶装置(1408)、表示系制御部(1410)、通信系制御部(1411)、その他 I/O 制御部(1412)が接続される。表示系制御部(1410)は、専用バスで主記憶装置制御部&システムバス制御部(1405)に接続されていても良い。外部記憶装置制御部(1408)には、外部記憶装置(1409)が接続される。

10 主記憶装置(1406)のアドレス領域と、システムバス(1407)に接続される各部分のアドレス領域は異なっているため、アドレスでアクセスすべき領域を判断し、主記憶装置制御部&システムバス制御部(1405)が切り替えている。

15 このような、情報処理装置(1401)では、情報処理装置を一つのシステムと捉えると、このシステム内の主となるプロセッサは、CPU(1402)である。この CPU 内部で暗号化処理を閉じさせる。例えば、CPU(1402)を第1図のように、マイクロプロセッサ(105)と、暗号処理アルゴリズム ROM(106)と、暗号処理ハードウェア(107)と、RAM(108)と、鍵保管領域(112)と、外部バス制御部(109)で構成し、さらに、同一半導体チップ上に集積する。また、本発明は、第19図および第20図に示すとおり、複数のCPUを有する情報処理装置であってもよい。

本発明の第五の実施例を第15図を用いて説明する。

25 第15図は、情報処理装置が他の情報処理装置と接続され、通信可能である構成を示す図である。ここでは、第1図の外部記憶装置の代わりに、

通信系制御部を設けた構成をとる。なお、通信系制御部は、情報処理装置の外に接続されていてもよい。

5 情報処理装置(1501)は、CPU(1502)と、通信系制御部(1503)とを備え、システムバス(1514)で接続される。CPU(1502)は、マイクロプロセッサ(1505)、暗号処理アルゴリズム ROM(1506)、暗号処理ハードウェア(1507)、RAM(1508)、外部バス制御部(1509)、鍵保管領域(1512)から構成され、マイクロプロセッサバス(1510)で接続される。

10 第15図では、情報処理装置は、CPUと通信系制御で構成されているが、他に主記憶や外部記憶装置等が備わっていても良い。通信系制御部(1503)を経由した通信回線(1504)の先に、外部記憶装置と同じ機能を持つ装置が接続されていても良いし、情報処理装置が接続されていても良い。

但し、通信回線(1504)の先に接続される装置が、記憶装置か情報処理装置かで、暗号の掛け方が異なる。

15 通信回線の先に接続される装置が、外部記憶装置の場合、データを暗号化し、それを記憶装置に格納し、暗号化されたデータを記憶装置から読み出して復号化するものである。このため、暗号化に用いた鍵は、暗号化を行った情報処理装置のCPUだけが保持していれば良い。

20 通信回線の先に接続される装置が、情報処理装置の場合、通信回線を挟んで情報処理装置Aと情報処理装置Bが存在する。この場合、情報処理装置Aで情報を暗号化し、情報処理装置Bで情報を復号化する状況が生ずる。大量のデータを高速に暗号化／復号化するためには、共通鍵暗号系が適する。しかし、暗号化と復号化で同じ鍵を用いるため、情報処理装置AとBで、同じ鍵を所有していなければならない。この同じ鍵を、情報処理装置AとBであらかじめ設定しておいても良いし、暗号化したデータを送る前に、情報処理装置AとBで相互認証を行い、暗号化に用いた鍵を共有する
25 方法を取っても良い。相互認証にも暗号処理が用いられるため、これらの

処理は、CPU 内部で処理される。

この情報処理装置 A と B がネットワークを介して接続されている様子を第 23 図に示す。

5 RAM(1508)内で、暗号化したデータを通信単位に再編集し、通信プロトコルに従い、通信系制御部(1503)に転送する事により、安全な通信が可能になる。RAM(1508)内で暗号化したデータを通信系制御部(1503)に転送し、通信系制御部(1503)において、暗号化したデータを通信単位に再編集し、通信プロトコルに従い、通信路(1504)にデータを送出しても良い。

10 本発明の第六の実施例を第 16 図、第 17 図、第 18 図、第 21 図および第 22 図を用いて説明する。

第 16 図は、磁気ディスク(1601)等の外部記憶装置群を、ディスクシステムコントローラ(1602)が制御する構成を取り、ディスクシステムコントローラ(1602)は、上位の情報処理装置であるホストシステム(1603)に接続されている。

15 磁気ディスク(1601)内には、ファイルとして記憶されているデータと、そのファイルが磁気ディスク上の何処に格納されているかを示すファイル配置情報がある。PC 等の小型情報処理装置では、ファイルとファイル配置情報を管理するファイルシステムプログラムを、小型情報処理装置の CPU が処理する場合もあるが、高速動作や高信頼性を実現するディスクシステムコントローラでは、ディスクシステムコントローラ自体がファイルと
20 ファイル配置情報を管理する場合もある。

本実施例は後者に適用したものである。ホストシステム(1603)では、ファイル(1604)とファイル識別子(1605)で管理する。ファイル(1604)が暗号化されてるか否かは、ホストシステムに依存し、ディスクシステムコントローラでは関知しなくて良い。ディスクシステムコントローラ(1602)では、磁気ディスク(1601)上のファイル配置情報(1606)を暗号化して管理す
25

る。

本実施例での、ホストシステムが暗号化した暗号化ファイル(1607)を読み出すまでの動作を説明する。

5 まず、ホストシステムは、必要とする暗号化ファイルに対応するファイル識別子(1605)をディスクシステムコントローラ(1602)に送り、暗号化ファイルの読み出し要求を行う。読み出し要求を受けたディスクシステムコントローラ(1602)は、磁気ディスク(1601)から、暗号化されたファイル配置情報(1606)を読み出し、ディスクシステムコントローラ(1602)内で復号化し、ファイル配置情報(1608)を取り出す。このファイル配置情報
10 (1608)内からファイル識別子(1605)を検索し、実際のファイルの配置情報を得る。選られたファイル配置情報を用いて、要求された暗号化ファイル(1607)を磁気ディスク(1601)から読み出し、ホストシステム(1603)へ転送する。

15 磁気ディスクにファイルを書き込む場合を第10図で説明する。ファイル配置情報(1608)を得るまでは、前記暗号化ファイルの読み出し動作と同じである。ファイル配置情報(1608)から、磁気ディスク(1601)の空き状態を確認し、磁気ディスク(1601)空き領域に暗号化ファイル(1604)を書き込む。書き込み終了後、ファイル配置情報(1608)を更新し、暗号化した後、磁気ディスク(1601)に暗号化ファイル配置情報(1701)として書き込む。

20 第18図で、ディスクシステムコントローラの構成を説明する。

 本発明のディスクシステムコントローラ(1801)は、内部にディスクシステムのCPU(1802)と、磁気ディスクインタフェース(1813)と、ホストシステムインタフェース(1804)を持ち、CPU(1802)は、マイクロプロセッサ(1805)と、暗号処理アルゴリズムROM(1806)と、暗号処理ハードウェア
25 (1807)と、RAM(1808)と、鍵保管領域(1811)と、外部バス制御部(1809)と、乱数生成器(1820)で構成される。

なお、第 2 1 図および第 2 2 図に示す通り、1 台の情報処理装置に複数の磁気ディスク装置が接続される構成としてもよい。

5 このような、ディスクシステムコントローラを用いる事により、磁気ディスク内の情報を全て暗号化する事が可能になり、情報保管時の安全性が高まる。

 本発明の暗号処理ハードウェアは、暗号化と復号化において共通の鍵を用いる共通鍵暗号では、専用のハードウェアであり、ローテータ、加算器、論理演算器等で構成される。共通鍵暗号としては、あるデータ長を単位に、ビットのローテートと加算と論理演算を主演算とした暗号化手段である
10 Multi 系の暗号、M6 暗号等を用いる事も出来る。

 公開鍵暗号を用いる場合は、演算量の大きい剰余演算器を専用のハードウェアとして設ける。

産業上の利用可能性

15 本発明によれば、情報処理装置内のシステムバスやプロセッサバスにも秘密情報を出さずに、暗号処理が可能になる。暗号処理とその処理に関する秘密情報、暗号アルゴリズム、途中経過、鍵情報等が、同一半導体内で処理されるため、秘密保持効果が高い情報処理装置を構築できる。

請 求 の 範 囲

1. 情報に対して所定の処理を施す制御装置と、
5 前記制御装置と当該情報処理装置を構成する他の装置を接続するバスを有する情報処理装置において、
前記制御装置は、鍵情報を生成し、暗号化すべき情報の暗号化を、当該制御装置を含む半導体チップ内で実行することを特徴とする情報処理装置。
2. 請求項 1 に記載の情報処理装置において、
10 前記制御装置は、暗号化されていない情報の前記バスへの出力を抑止する外部バス制御装置を有することを特徴とする情報処理装置。
3. 請求項 2 に記載の情報処理装置において、
前記外部バス制御装置は、暗号化しなくともよい情報は、前記バスへ出力することを特徴とする情報処理装置。
- 15 4. 請求項 1 に記載の情報処理装置において、
前記制御装置で暗号化された情報を格納する記憶装置を有することを特徴とする情報処理装置。
5. 請求項 1 に記載の情報処理装置において、
20 前記制御装置は、情報の書き込みの際に、暗号化された情報を復号化する手段を有することを特徴とする手段を有することを特徴とする情報処理装置。
6. 請求項 5 に記載の情報処理装置において、
ネットワークを介して他の情報処理装置と接続され、他の情報処理装置で暗号化されて送信された情報を前記制御装置で復号化することを特徴とする情報処理装置。
- 25 7. 請求項 1 に記載の情報処理装置において、

前記処理装置を複数個有し、夫々の処理装置にて暗号化を行うことを特徴とする情報処理装置。

8. 請求項1に記載の情報処理装置において、

5 前記処理装置は、暗号化されたプログラムを受信し、復号化を施す手段を有することを特徴とする情報処理装置。

9. 請求項1に記載の情報処理装置において、

前記処理装置は、前記所定の処理を実行するマイクロプロセッサと、
前記情報の暗号化処理のアルゴリズムが格納された暗号処理アルゴリズム格納装置と、

10 前記アルゴリズムに従って暗号化処理を実行する暗号化装置と、
前記マイクロプロセッサ、暗号処理アルゴリズム格納装置および前記暗号化装置それぞれを接続するマイクロプロセッサバスと
を有することを特徴とする情報処理装置。

15 10. 情報を処理する処理装置を有し、暗号化された暗号化情報を格納する磁気ディスクを制御するディスクシステムコントローラにおいて、

前記暗号化情報の読み出し要求を受け取った場合、鍵情報を生成し、前記磁気ディスクに格納された情報の配置を示す暗号化されている暗号化ファイル配置情報を、前記磁気ディスクから読み出し、読み出した暗号化ファイル配置情報を前記処理装置を含む半導体チップ内で復号化し、復号化されたファイル配置情報に基づいて、前記暗号化情報を読み出すことを特徴とするディスクシステムコントローラ。

11. 請求項10に記載ディスクシステムコントローラにおいて、

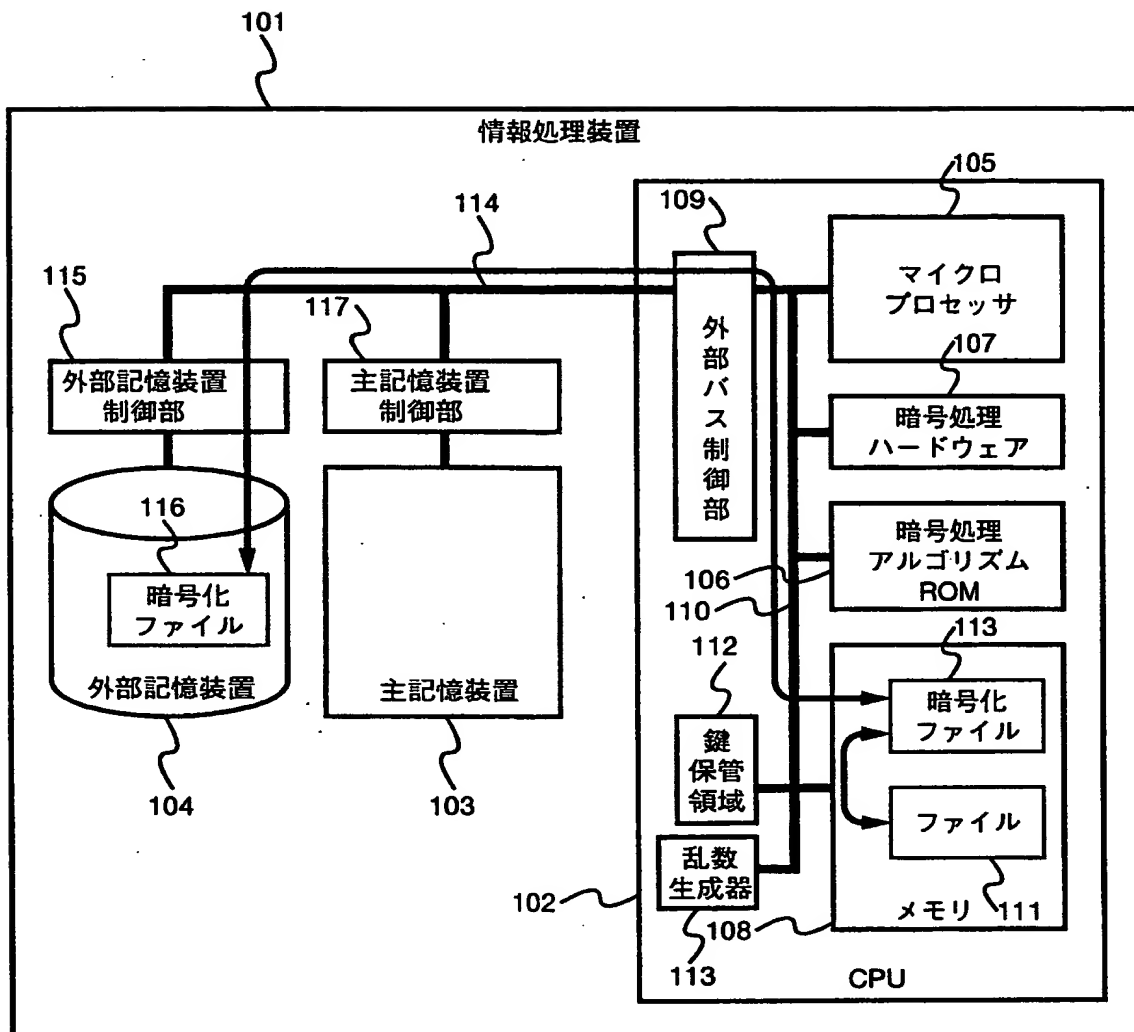
当該ディスクコントローラは、複数の磁気ディスクに接続されていることを特徴とするディスクシステムコントローラ。

25 12. 請求項10に記載ディスクシステムコントローラにおいて、

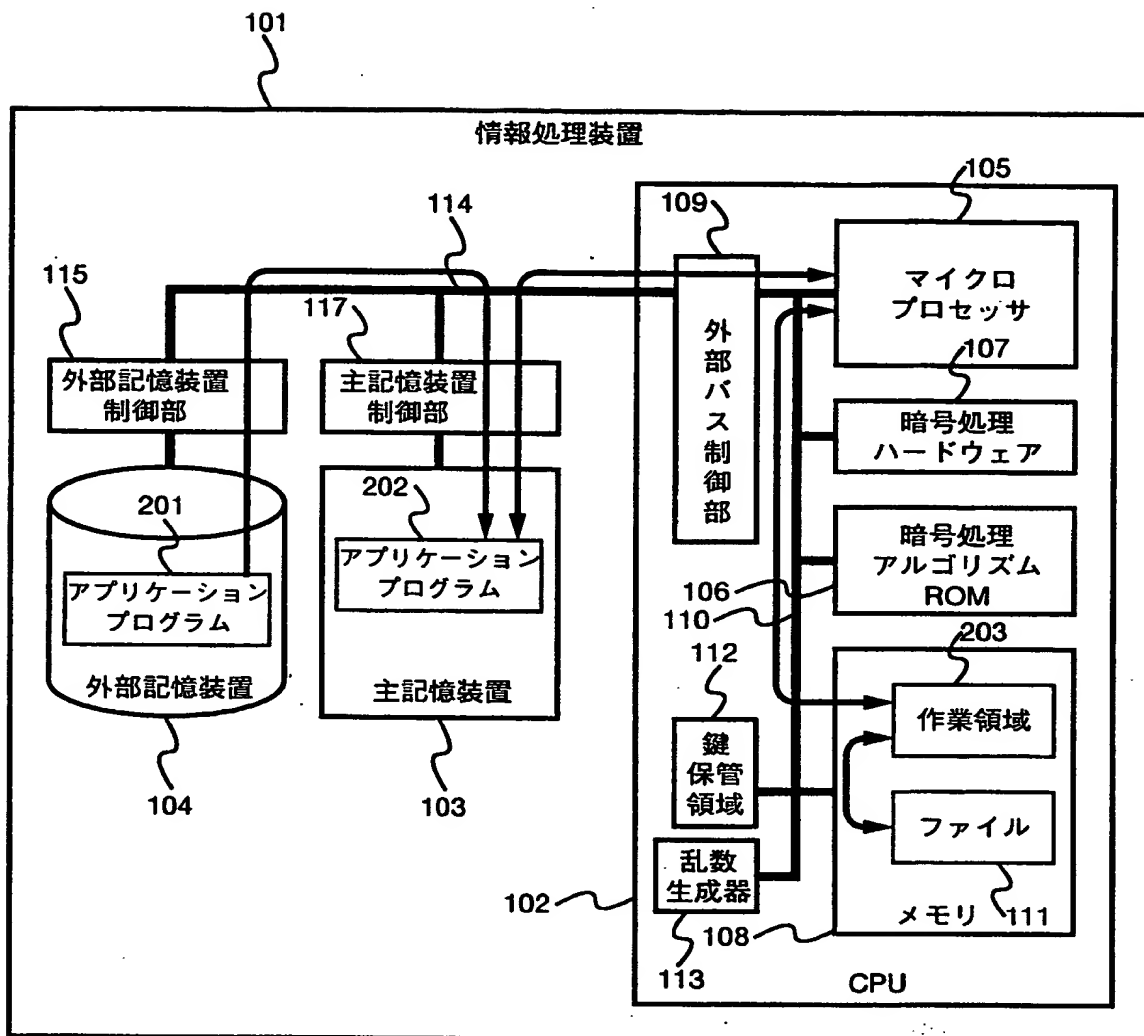
当該ディスクシステムコントローラは、情報処理装置に接続されており、

前記情報処理装置からの要求により、前記暗号化情報を読み出すことを特徴とするディスクシステムコントローラ。

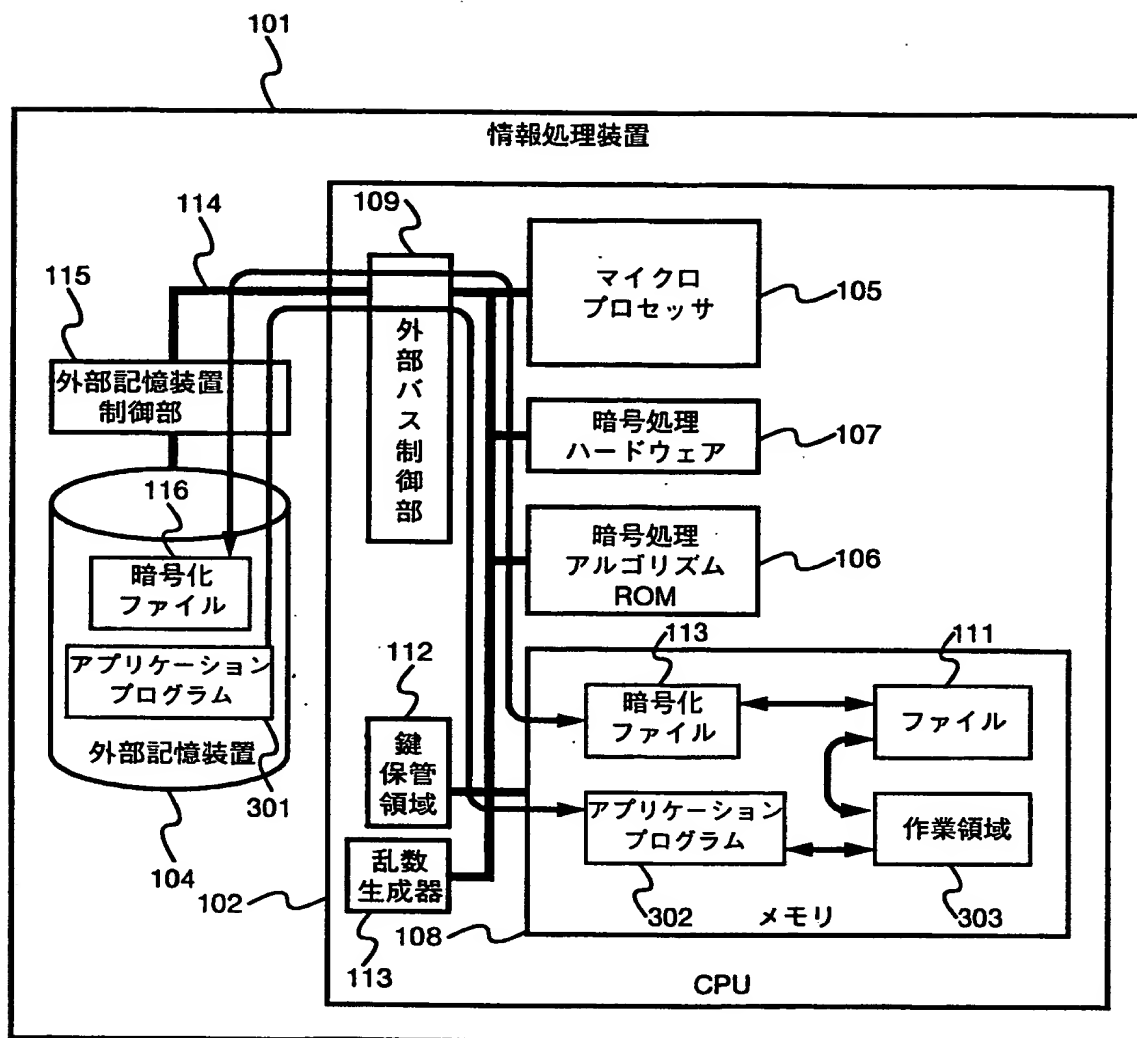
第1図



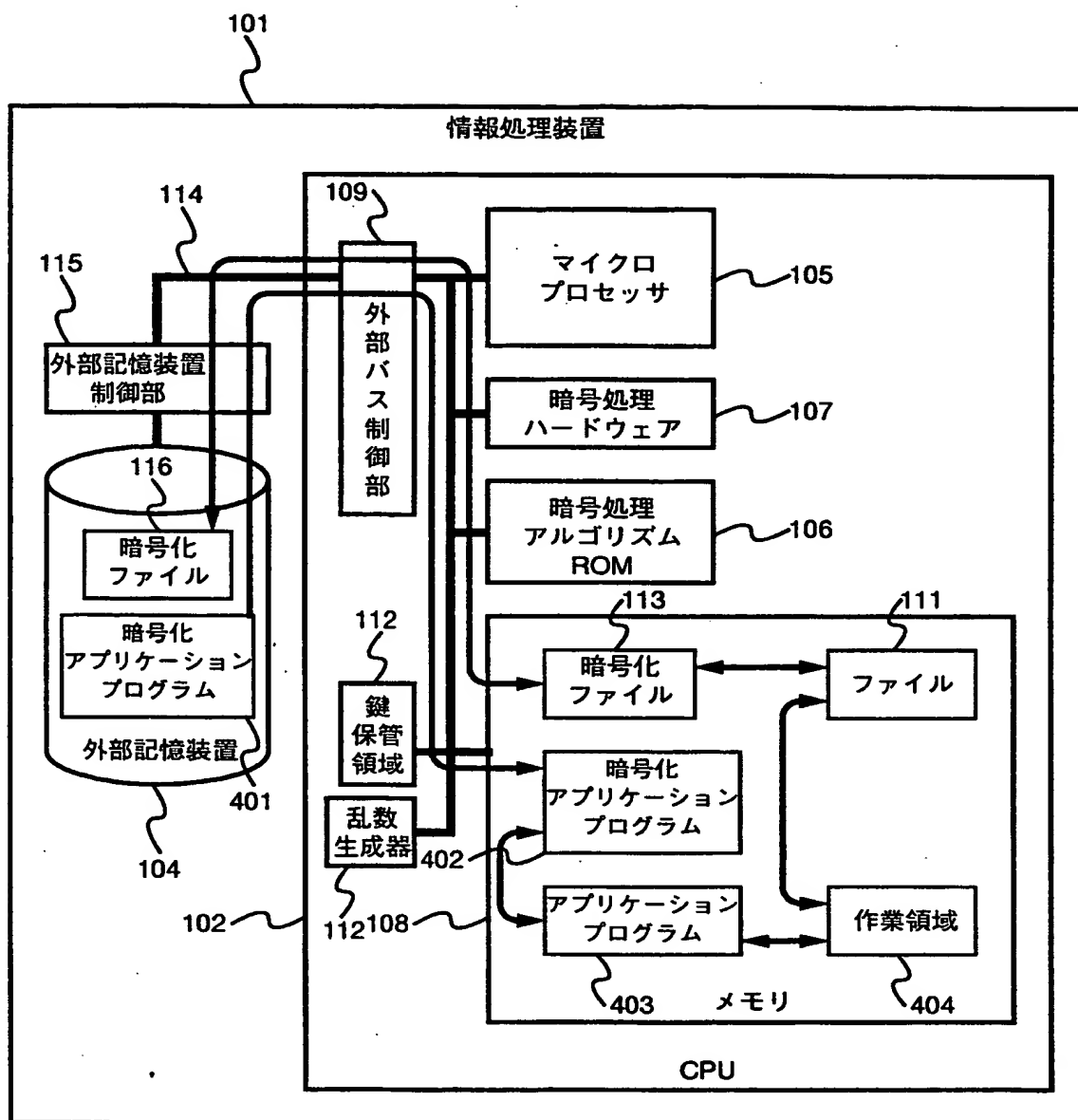
第2図



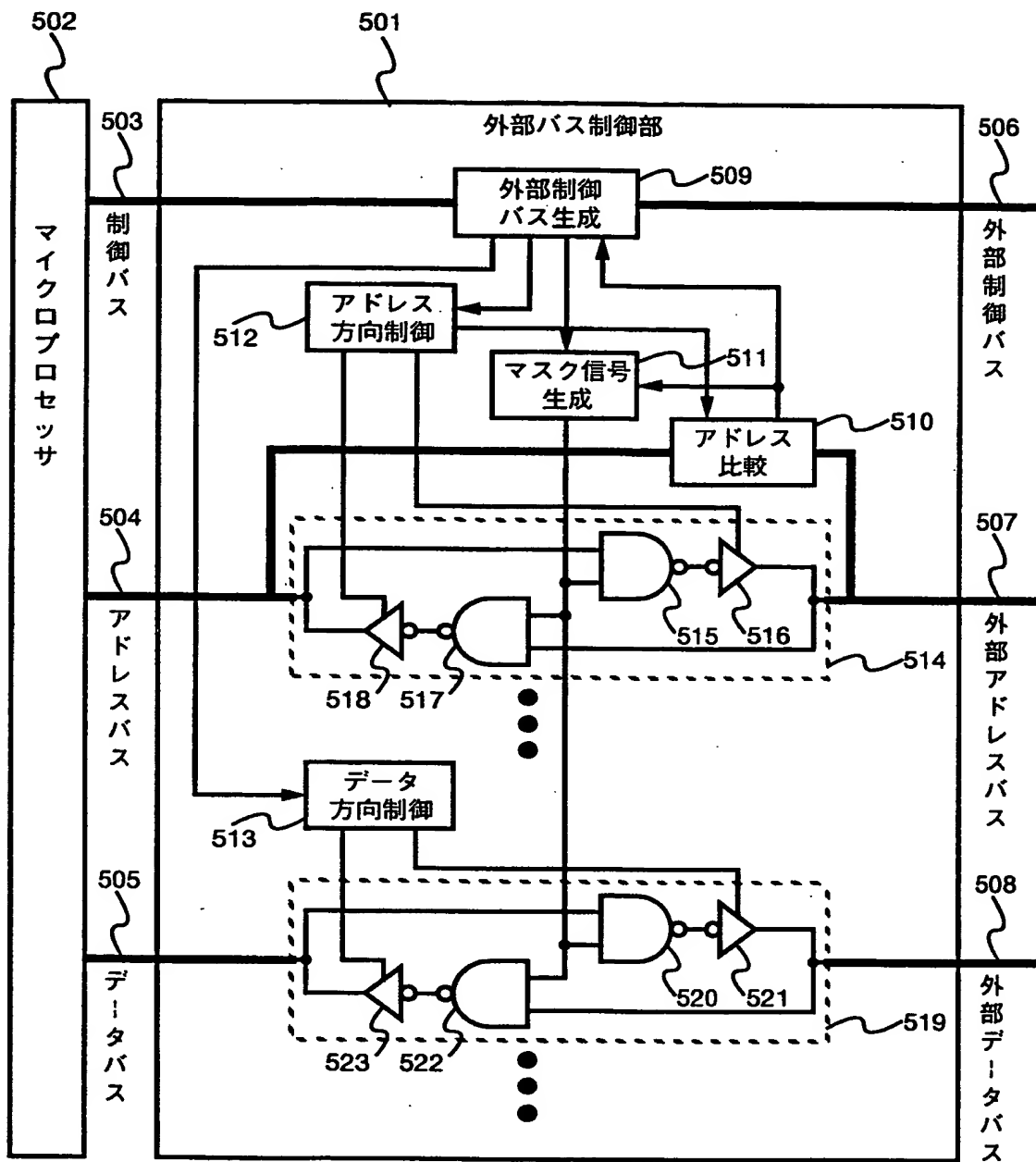
第3図



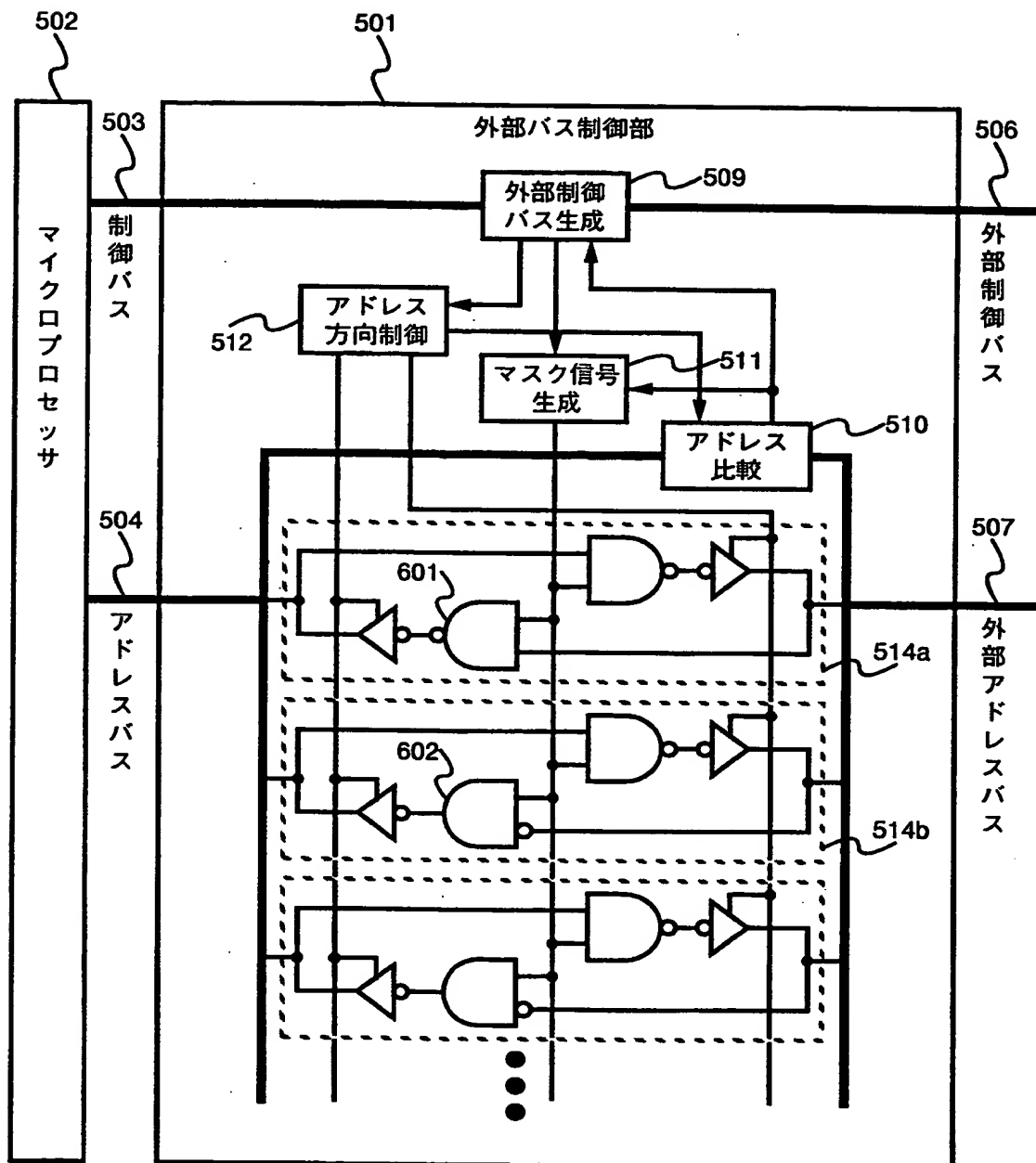
第4図



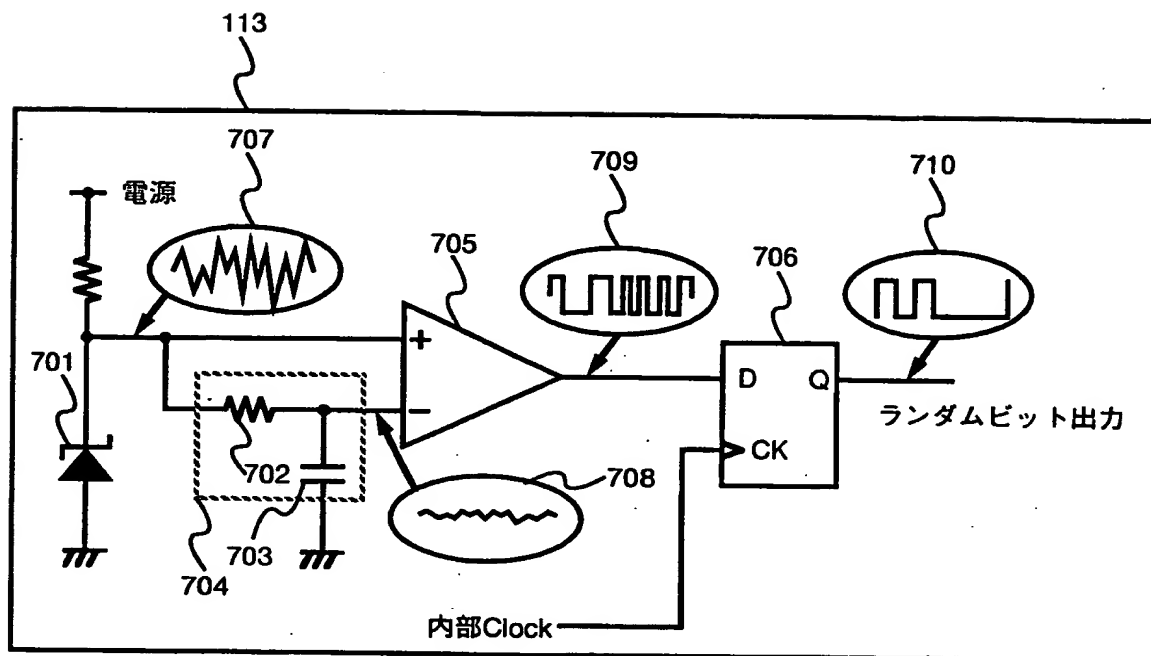
第5図



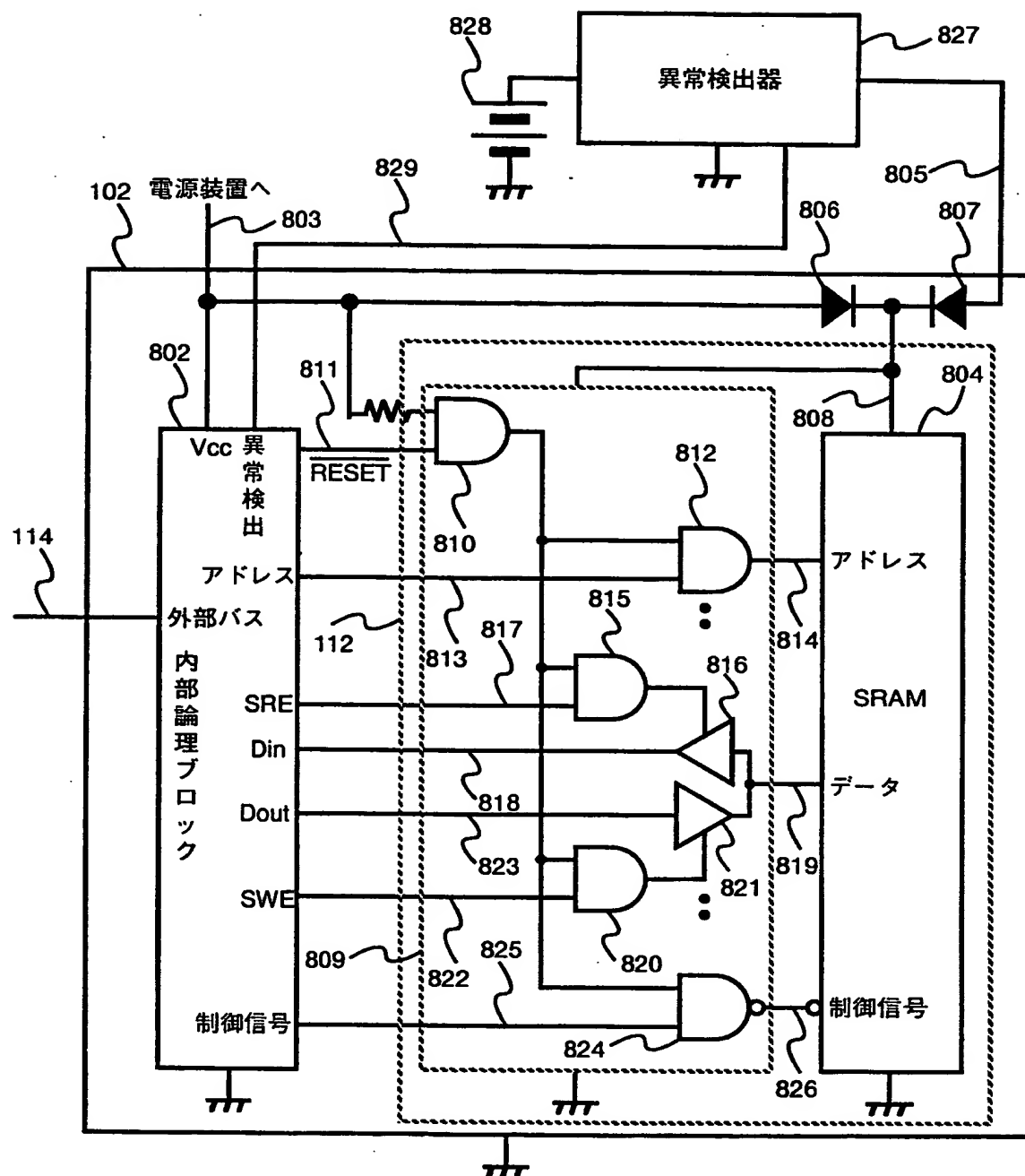
第 6 図



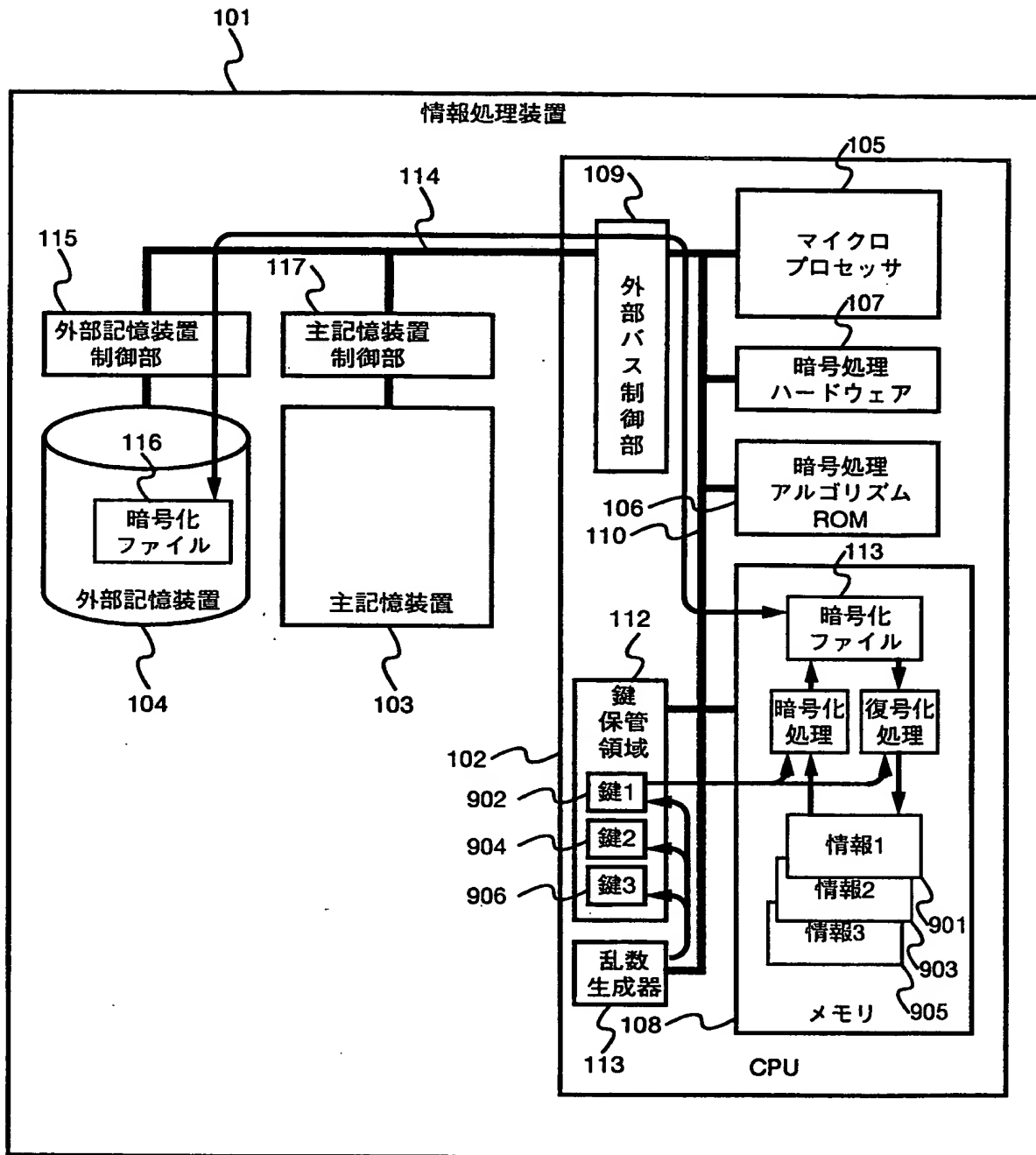
第 7 図



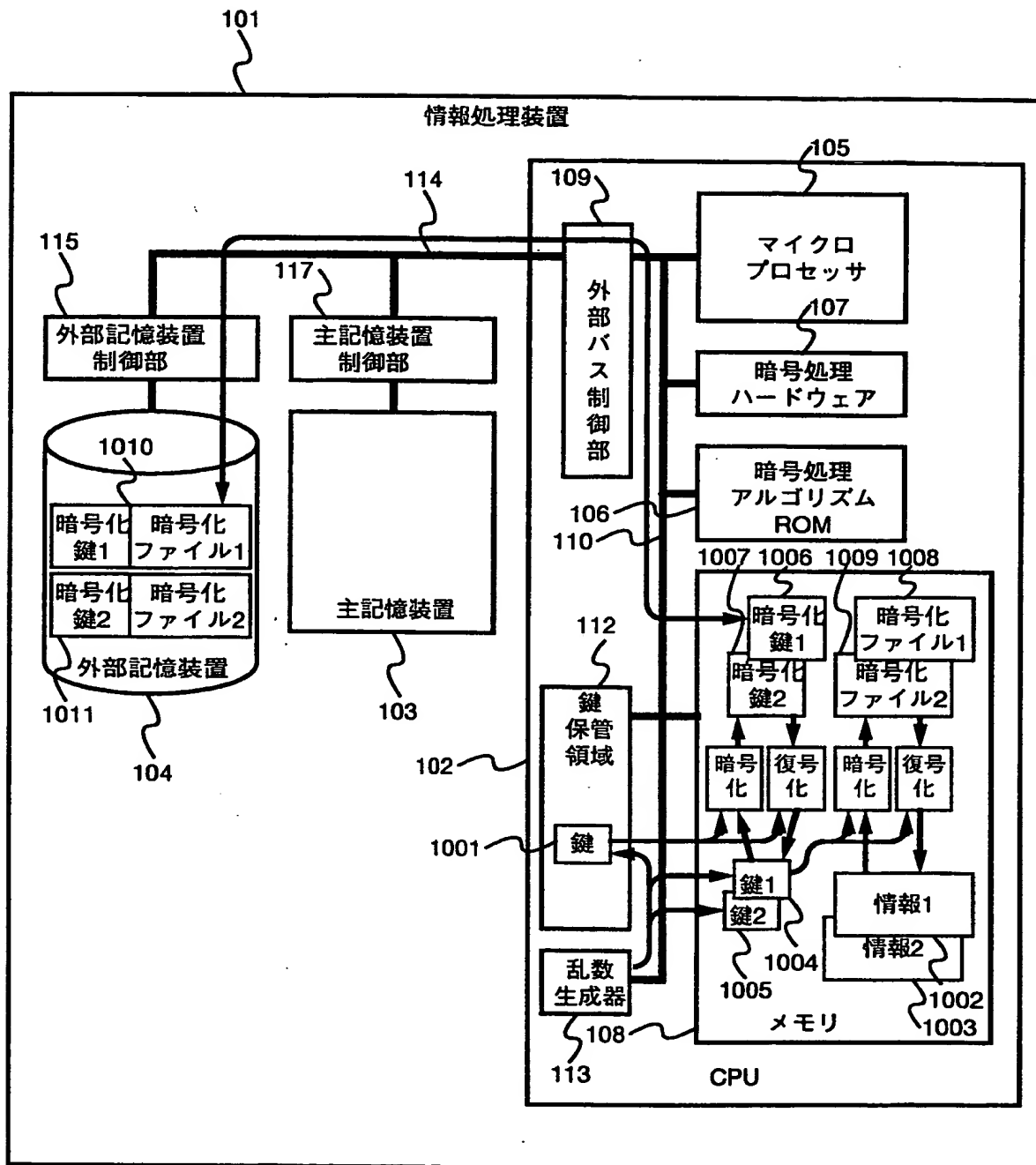
第 8 図



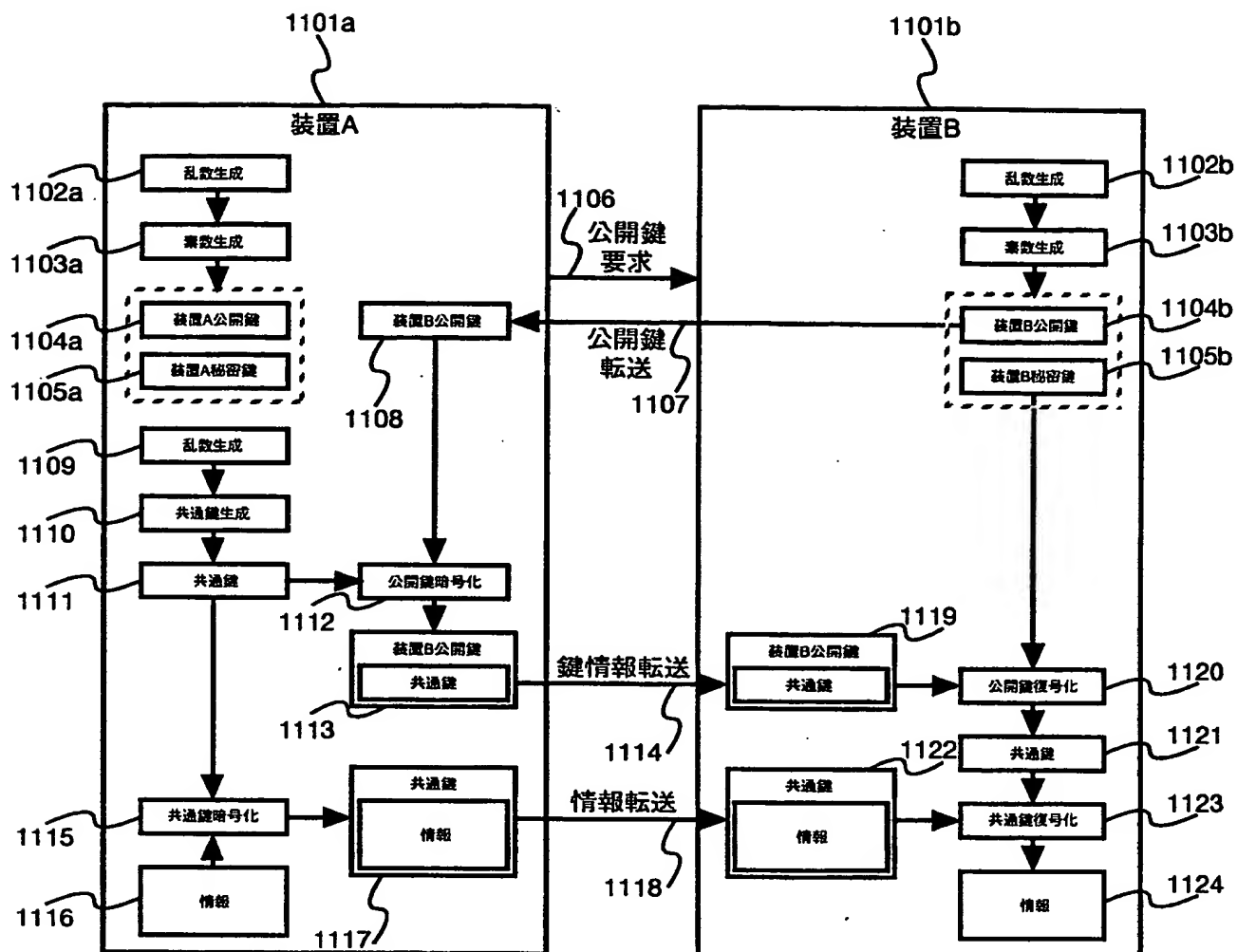
第9図



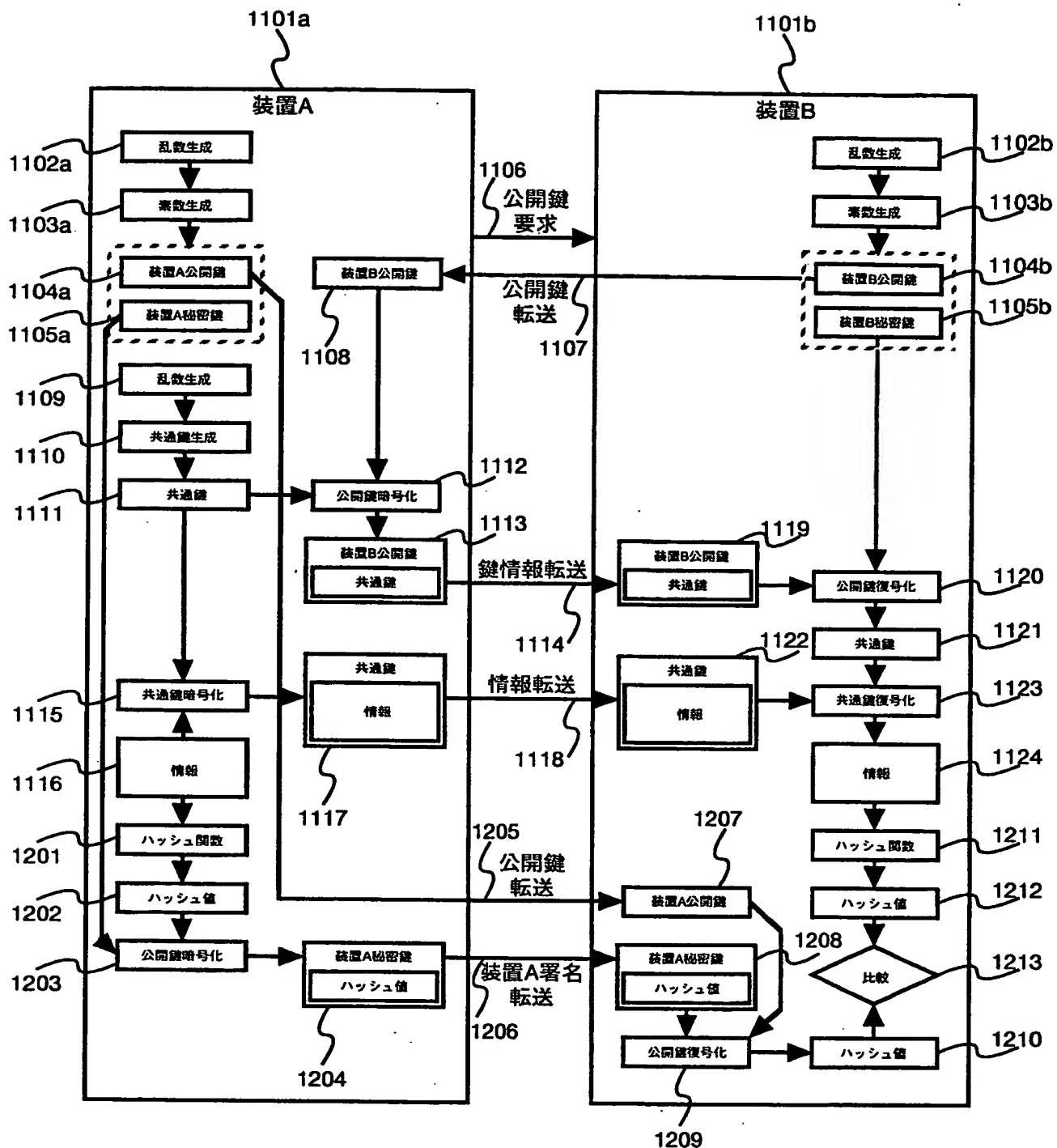
第10図



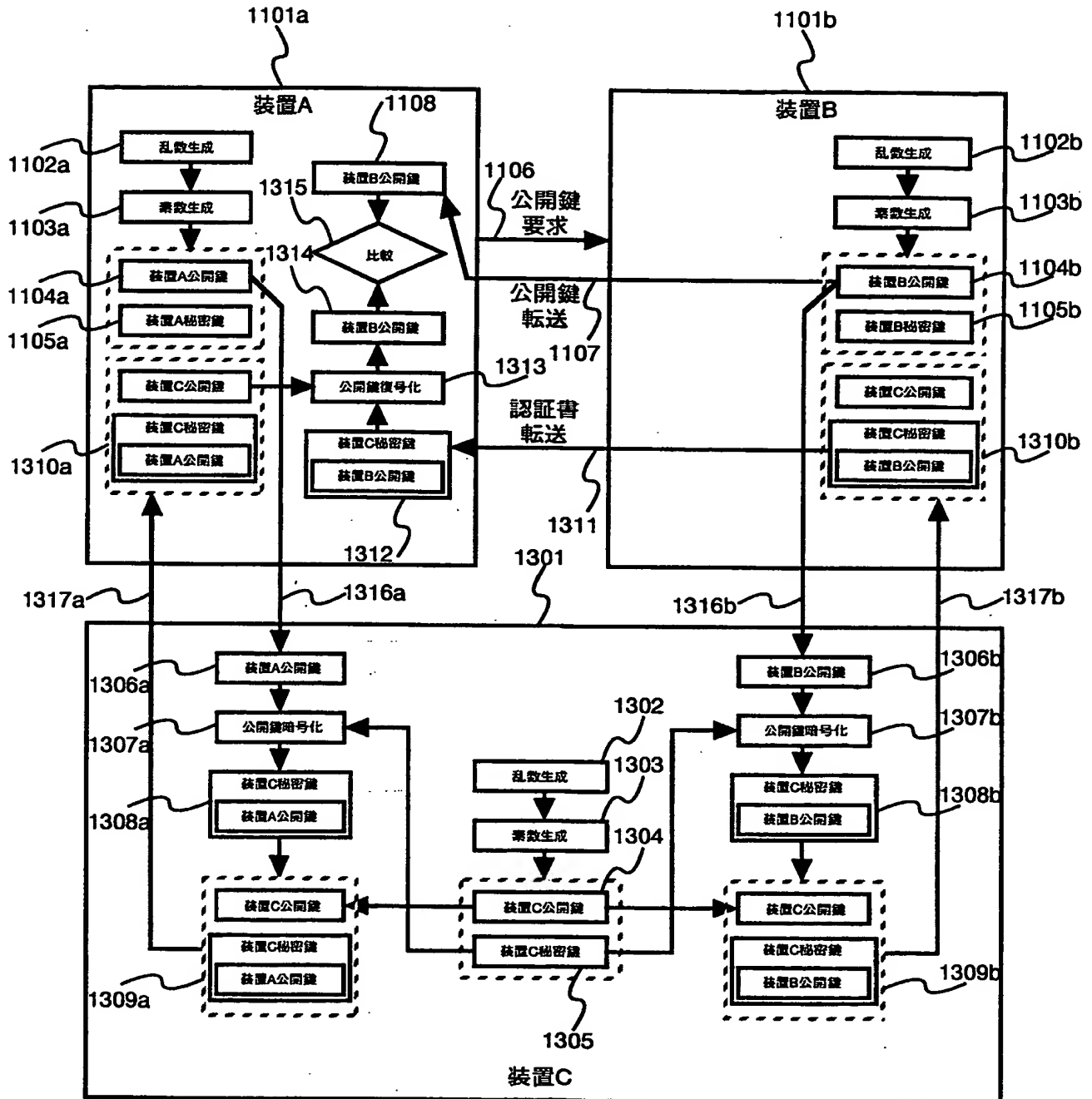
第 1 1 図



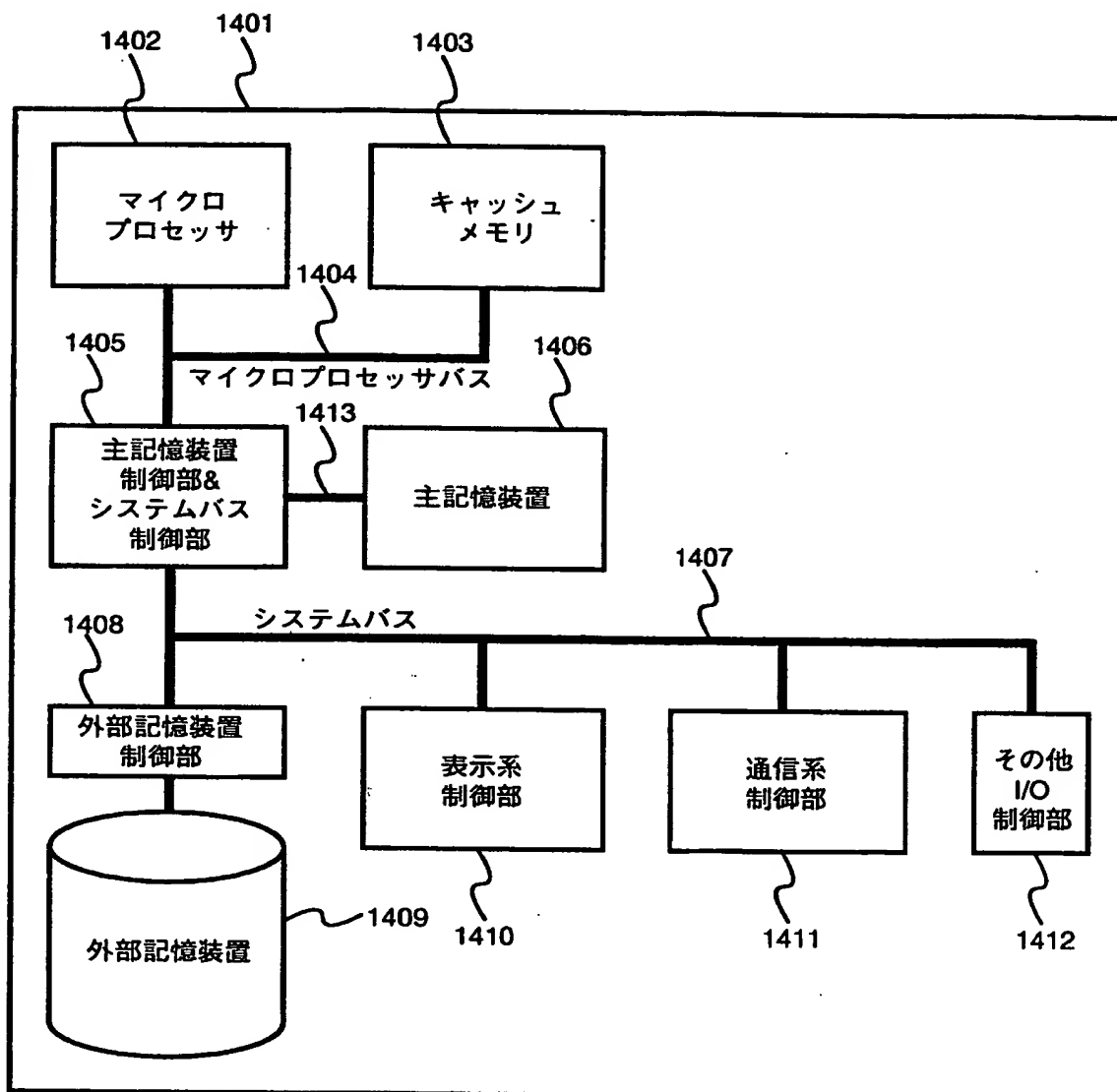
第12図



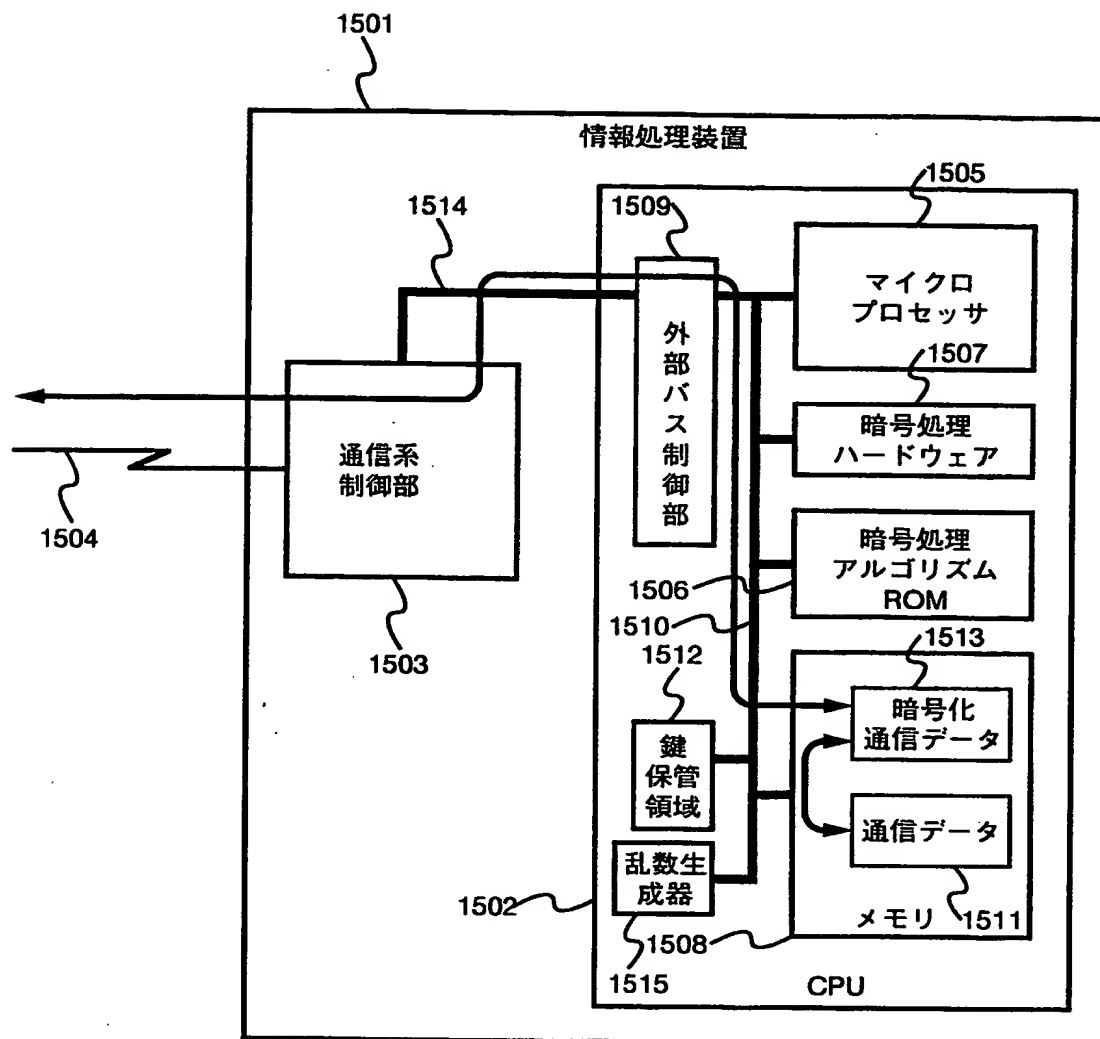
第 1 3 図



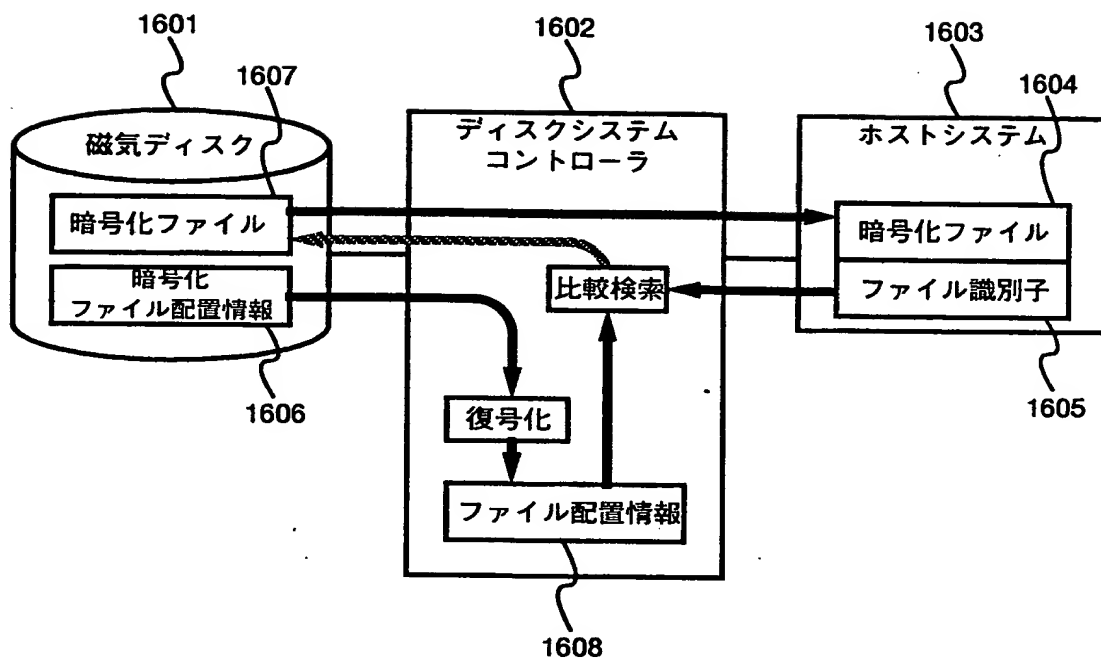
第 1 4 図



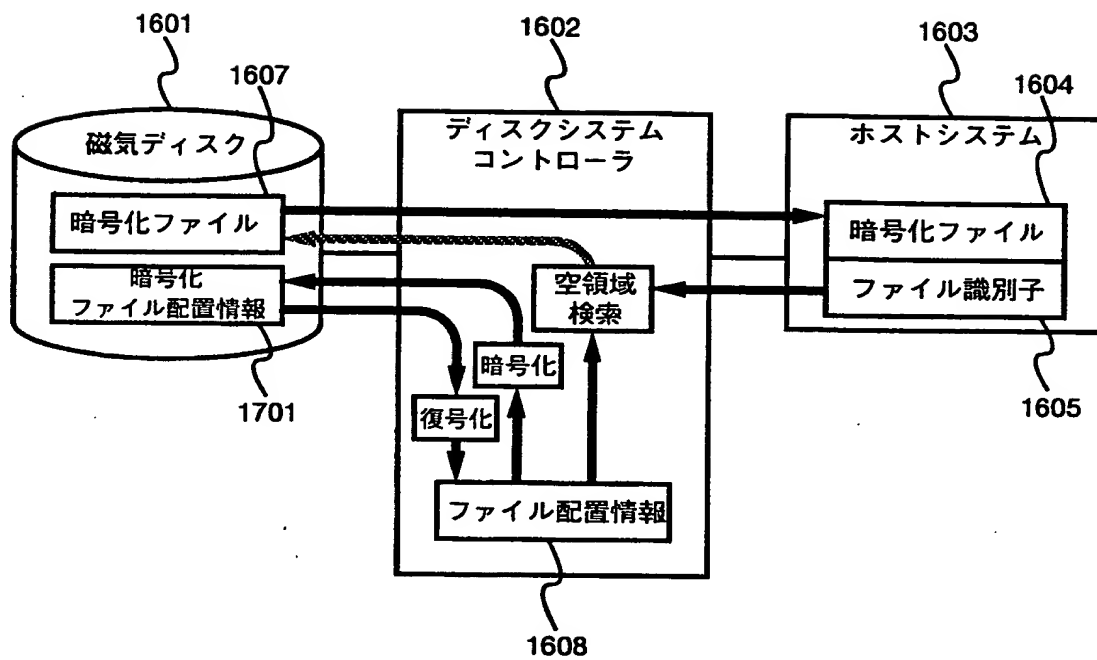
第15図



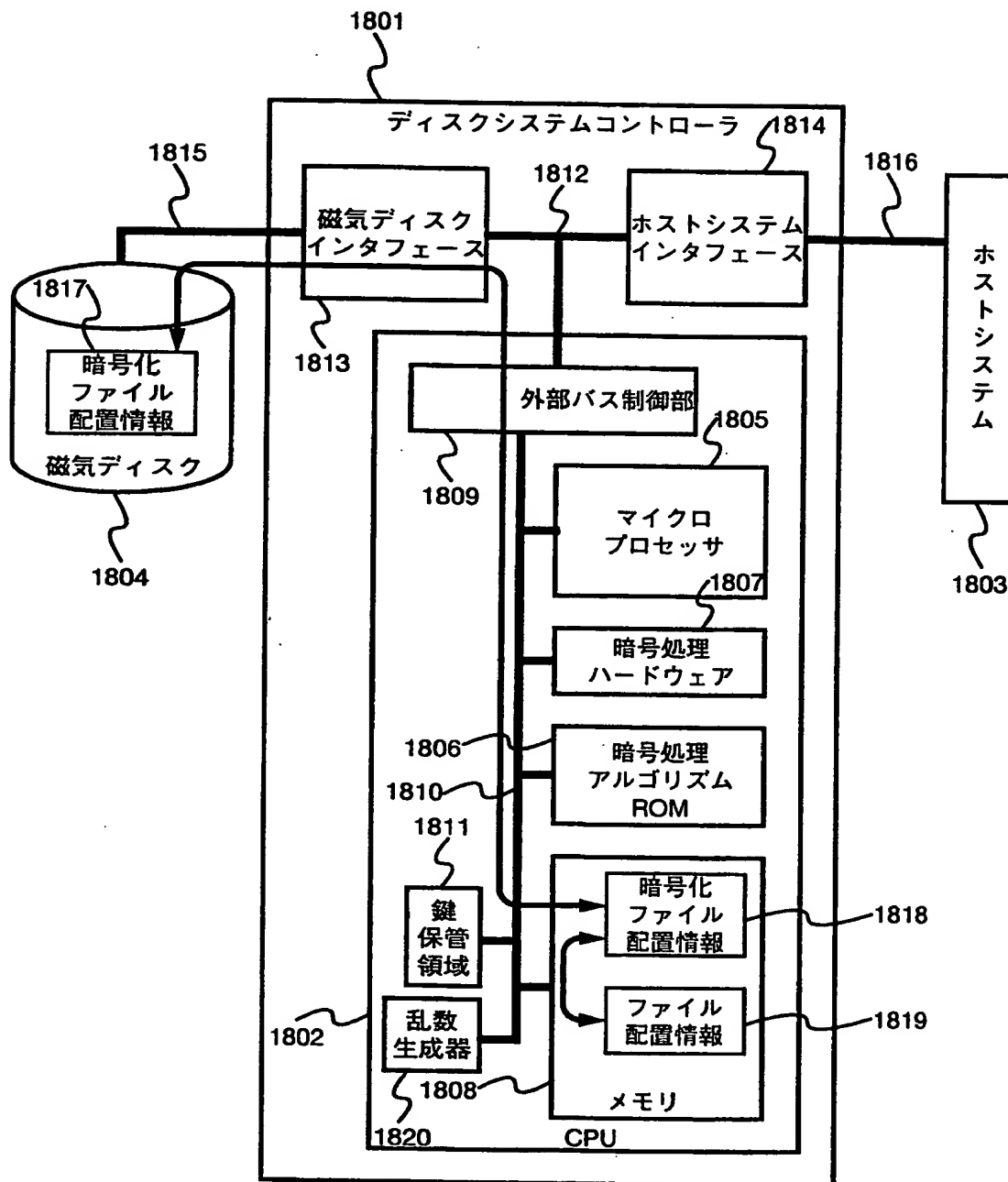
第 1 6 図



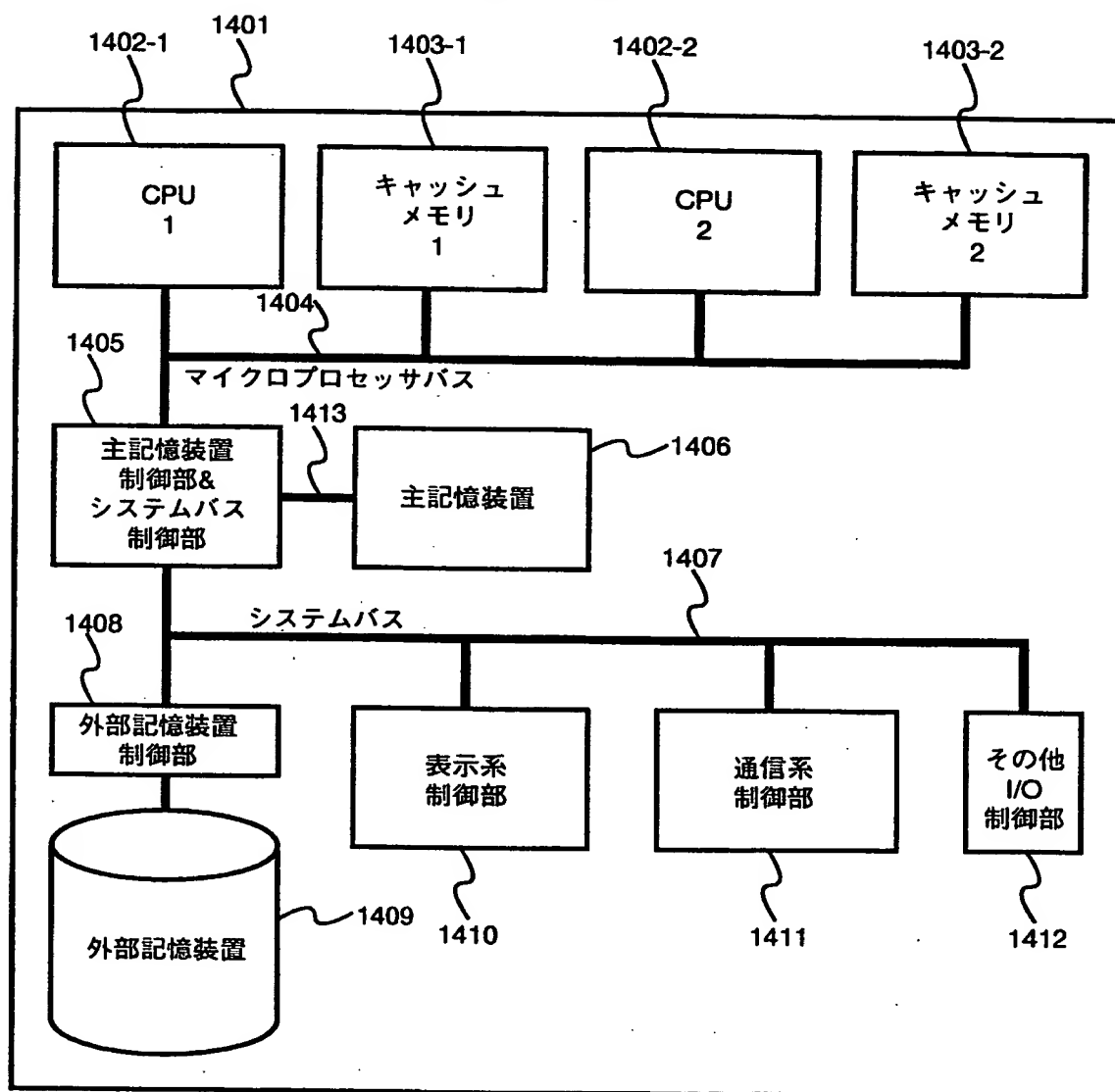
第 17 図



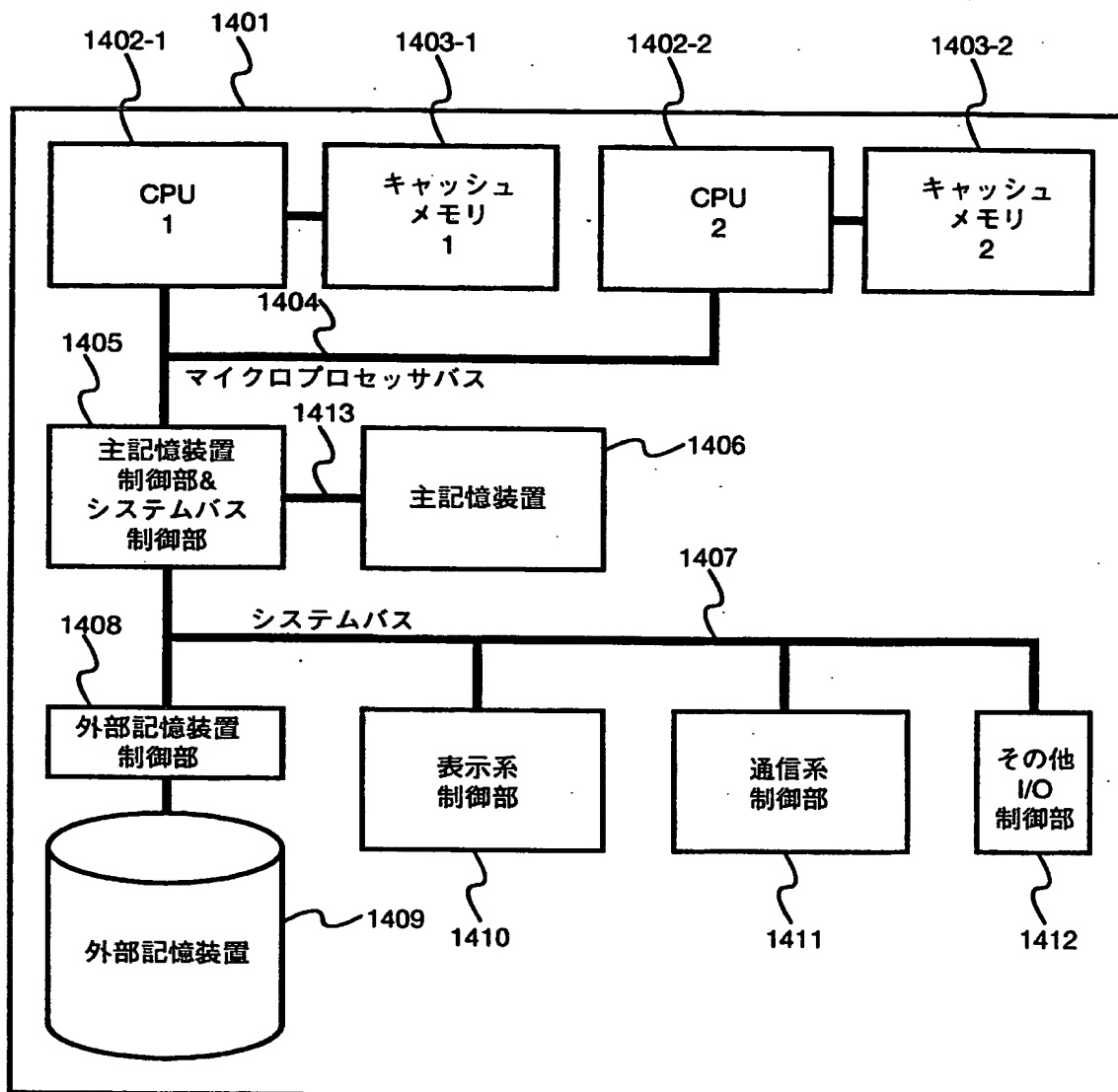
第 1 8 図



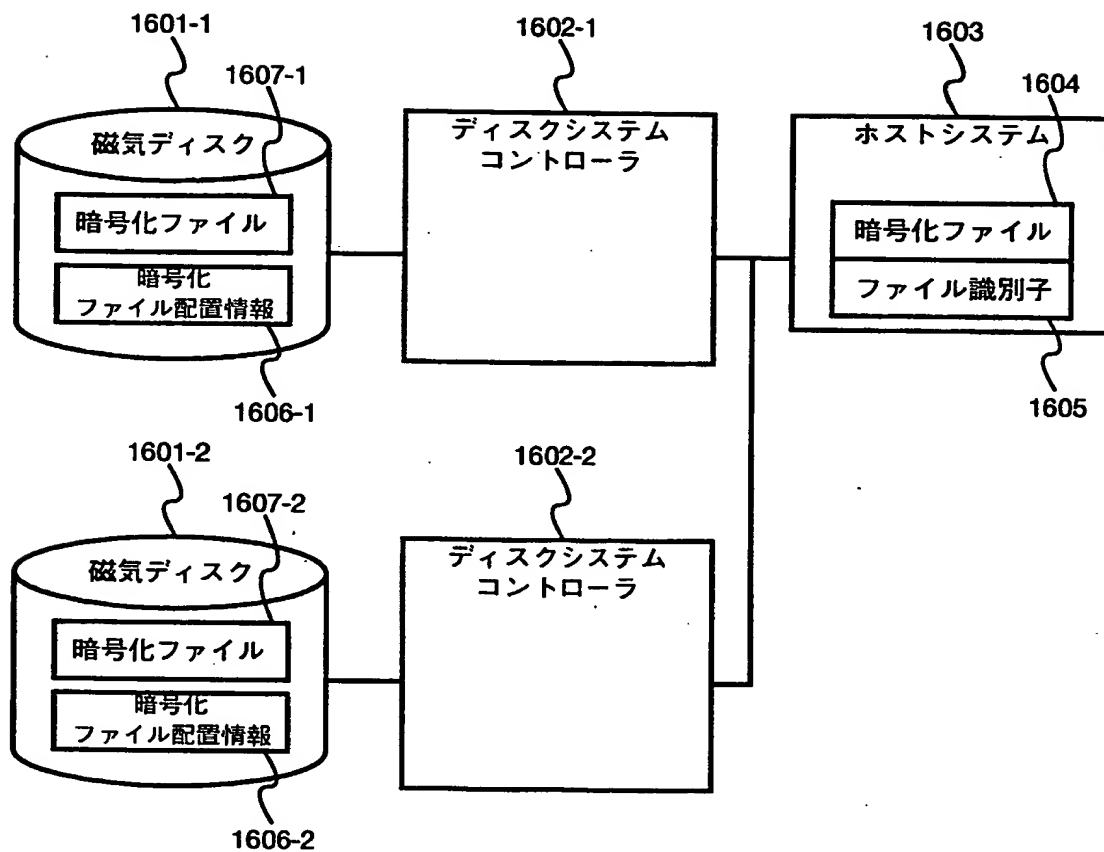
第 1 9 図



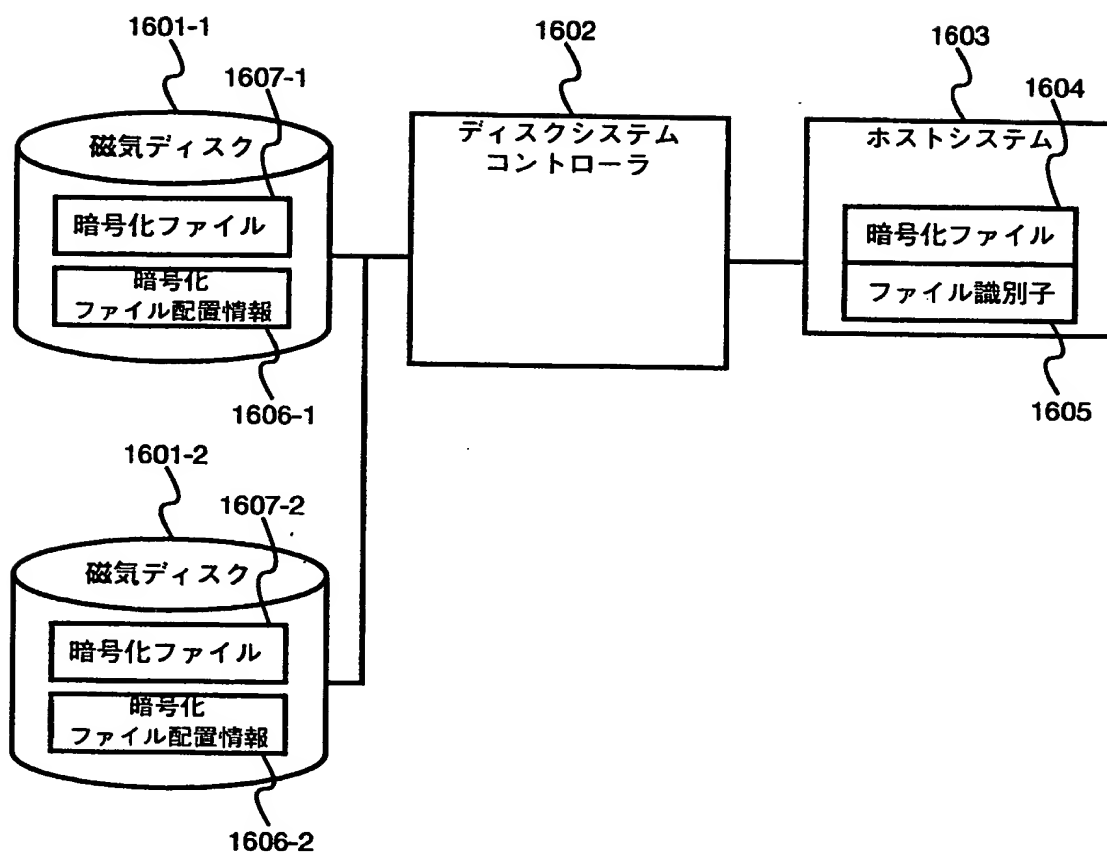
第 20 図



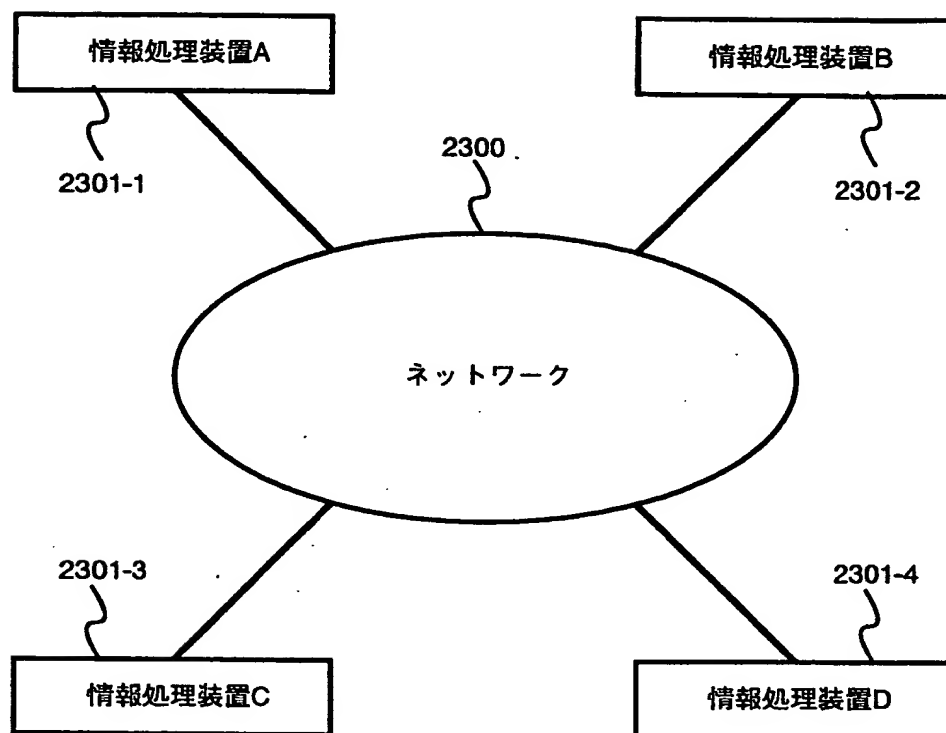
第 2 1 図



第 2 2 図



第 2 3 図



国際調査報告

国際出願番号 PCT/JP00/01333

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, G06F15/78, G06F3/06, G11B20/10

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, G06F15/78, G06F3/06, G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996
 日本国実用新案登録公報 1996-2000
 日本国公開実用新案公報 1971-2000

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y	J P, 05-053921, A (新日本製鐵株式会社) 5. 3月. 1993 (05. 03. 93), (ファミリーなし)	1-9 10-12
X Y	J P, 64-041947, A (株式会社日立製作所, 日立東部 セミコンダクタ株式会社) 14. 2月. 1989 (14. 02. 89), (ファミリーなし)	1-9 10-12
Y	J P, 04-163768, A (株式会社日立製作所) 9. 6月. 1992 (09. 06. 92), (ファミリーなし)	10-12

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」口頭による開示、使用、展示等に言及する文献
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

19. 05. 00

国際調査報告の発送日

13.06.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

梅村 勁 樹

5N

7313

電話番号 03-3581-1101 内線 3545

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, 09-044407, A (日本電気エンジニアリング株式会社) 14. 2月. 1997 (14. 02. 97), (ファミリーなし)	10-12
A	JP, 04-149652, A (三菱電機株式会社) 22. 5月. 1992 (22. 05. 92), (ファミリーなし)	1-12
A	JP, 02-297626, A (日本電気株式会社) 10. 12月. 1990 (10. 12. 90), (ファミリーなし)	1-9
A	JP, 05-314014, A (株式会社東芝) 26. 11月. 1993 (26. 11. 93), (ファミリーなし)	10-12

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/01333

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F12/14, G06F15/78, G06F3/06, G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F12/14, G06F15/78, G06F3/06, G11B20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Kokai Jitsuyo Shinan Koho 1971-2000

Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP, 05-053921, A (Nippon Steel Corporation), 05 March, 1993 (05.03.93) (Family: none)	1-9 10-12
X Y	JP, 64-041947, A (Hitachi, Ltd., Hitachi Tobu Semiconductor K.K.), 14 February, 1989 (14.02.89) (Family: none)	1-9 10-12
Y	JP, 04-163768, A (Hitachi, Ltd.), 09 June, 1992 (09.06.92) (Family: none)	10-12
Y	JP, 09-044407, A (NEC Eng. Ltd.), 14 February, 1997 (14.02.97) (Family: none)	10-12
A	JP, 04-149652, A (Mitsubishi Electric Corporation), 22 May, 1992 (22.05.92) (Family: none)	1-12
A	JP, 02-297626, A (NEC Corporation), 10 December, 1990 (10.12.90) (Family: none)	1-9
A	JP, 05-314014, A (Toshiba Corporation), 26 November, 1993 (26.11.93) (Family: none)	10-12

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
19 May, 2000 (19.05.00)Date of mailing of the international search report
13 June, 2000 (13.06.00)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

PCT

国際調査報告

(法8条、法施行規則第40、41条)
[PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号 00267971	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)及び下記5を参照すること。		
国際出願番号 PCT/JP00/01333	国際出願日 (日.月.年) 06.03.00	優先日 (日.月.年) 19.03.99	
出願人(氏名又は名称) 株式会社 日立製作所			

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 3 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☐ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 1 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, G06F15/78, G06F3/06, G11B20/10

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, G06F15/78, G06F3/06, G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996
 日本国実用新案登録公報 1996-2000
 日本国公開実用新案公報 1971-2000

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y	JP, 05-053921, A (新日本製鐵株式会社) 5. 3月. 1993 (05. 03. 93), (ファミリーなし)	1-9 10-12
X Y	JP, 64-041947, A (株式会社日立製作所, 日立東部 セミコンダクタ株式会社) 14. 2月. 1989 (14. 02. 89), (ファミリーなし)	1-9 10-12
Y	JP, 04-163768, A (株式会社日立製作所) 9. 6月. 1992 (09. 06. 92), (ファミリーなし)	10-12

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

19. 05. 00

国際調査報告の発送日

13.06.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

梅村 勁樹

5N

7313

電話番号 03-3581-1101 内線 3545

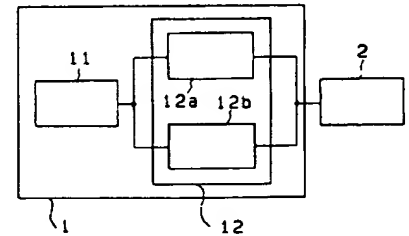
C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y・	J P, 09-044407, A (日本電気エンジニアリング株式会社) 14. 2月. 1997 (14. 02. 97), (ファミリーなし)	10-12
A	J P, 04-149652, A (三菱電機株式会社) 22. 5月. 1992 (22. 05. 92), (ファミリーなし)	1-12
A	J P, 02-297626, A (日本電気株式会社) 10. 12月. 1990 (10. 12. 90), (ファミリーなし)	1-9
A	J P, 05-314014, A (株式会社東芝) 26. 11月. 1993 (26. 11. 93), (ファミリーなし)	10-12

(54) INTEGRATED CIRCUIT

(11) 5-53921 (A) (43) 5.3.1993 (19) JP
 (21) Appl. No. 3-237147 (22) 23.8.1991
 (71) NIPPON STEEL CORP (72) YUZURU SASAKI(2)
 (51) Int. Cl.⁵ G06F12/14, G06F15/78, G09C1/00

PURPOSE: To prevent data and circuit functions from being copied at an integrated circuit for inputting/outputting data while being connected to an external circuit.

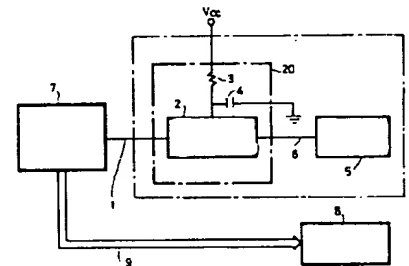
CONSTITUTION: An integrated circuit 1 is equipped with a main circuit 11 to realize the main function and a ciphering/deciphering circuit 12. The ciphering/deciphering circuit 12 is equipped with a ciphering circuit 12a, which ciphers the data outputted from the main circuit 11 and outputs the data to the external circuit 2, and a deciphering circuit 12b to decipher the ciphered data inputted from the outside circuit 2 and to output the data to the main circuit 11. Even when the data inputted/outputted to/from the integrated circuit 1 are copied, the data can not be used at a circuit copying only the function of the main circuit 11. Since the data are ciphered, it is also difficult to copy the main circuit 11.

**(54) MEMORY CARD ACCESS DEVICE**

(11) 5-53922 (A) (43) 5.3.1993 (19) JP
 (21) Appl. No. 3-218775 (22) 29.8.1991
 (71) NEC CORP(1) (72) HIDEO SAKAMOTO(1)
 (51) Int. Cl.⁵ G06F12/16, G06K17/00

PURPOSE: To report the access of a memory card to a user without fail.

CONSTITUTION: When a memory card control signal 9 is transmitted from a central processing unit 7 to a memory card 8 and the state of the memory card control signal 9 reads or writes the memory card 8, a memory card access signal 1 is made effective and this memory card access signal 1 is inputted to a one-shot multivibrator 2 and inputted to an access display device 5 while extending an access display signal 6 only for time decided by a resistor 3 and a capacitor 4 so as to report it to the user that the memory card 8 is under access. Since the access of the memory card 8 is not displayed by a software, the access of the memory card 8 can be reported to the user without fail and since it can be set by a hardware to use the memory card 8 longer than real using time, the memory card 8 can be loaded/unloaded safely.



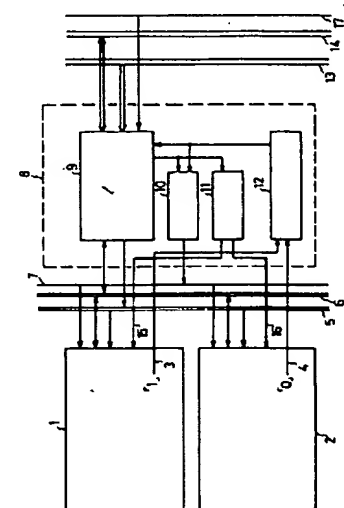
20: access display signal generating means, (a): memory card access device

(54) MAIN STORAGE DEVICE CONTROL CIRCUIT

(11) 5-53923 (A) (43) 5.3.1993 (19) JP
 (21) Appl. No. 3-233796 (22) 22.8.1991
 (71) NEC CORP (72) AKIRA SEKIGUCHI
 (51) Int. Cl.⁵ G06F12/16, G06F12/06

PURPOSE: To realize the main storage device control circuit for controlling plural memory cards having different access speed in common.

CONSTITUTION: For the unit of memory cards 1 and 2, the access speed information of the used semiconductor memory cell is provided and transmitted to a timing control circuit 12 in a main storage device control circuit 8 by individual access speed information lines 3 and 4 and corresponding to the accessed memory cards 1 and 2, this timing control circuit 12 executes timing control to an address/data control circuit 9 and a memory bus control signal transmission circuit 10 so as to realize a write/read operation at speed corresponding to a memory board.



11: board select signal transmission circuit

Best Available Copy

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平5-53921

(43)公開日 平成5年(1993)3月5日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0 B	9293-5B		
15/78	5 1 0 Z	7530-5L		
G 0 9 C 1/00		7922-5L		

審査請求 未請求 請求項の数3(全 7 頁)

(21)出願番号 特願平3-237147

(22)出願日 平成3年(1991)8月23日

(71)出願人 000006655

新日本製鐵株式会社

東京都千代田区大手町2丁目6番3号

(72)発明者 佐々木 譲

東京都千代田区大手町2-6-3 新日本
製鐵株式会社内

(72)発明者 柴田 高幸

東京都千代田区大手町2-6-3 新日本
製鐵株式会社内

(72)発明者 成田 喜則

東京都千代田区大手町2-6-3 新日本
製鐵株式会社内

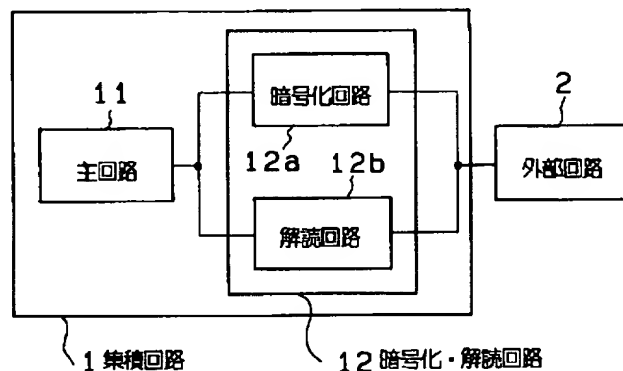
(74)代理人 弁理士 國分 孝悦

(54)【発明の名称】 集積回路

(57)【要約】

【目的】 外部回路と接続されてデータの入出力を行う集積回路において、データの複製および回路の機能の複製を防止する。

【構成】 集積回路1に、主たる機能を実現する主回路11、暗号化解読回路12を設けた。暗号化解読回路12は、主回路11から出力されたデータを暗号化し外部回路2へ出力する暗号化回路12aと外部回路2から入力された暗号化されたデータを解読し主回路11へ出力する解読回路12bを有している。集積回路1に入出力されるデータを複製しても主回路11の機能のみを複製した回路では使用できない。また、データが暗号化されているため、主回路の複製も困難である。



【特許請求の範囲】

【請求項 1】 外部装置との間でデータの入出力が行われ、該入出力されるデータを処理する集積回路において、該集積回路は、前記集積回路の機能に基づく種々の動作を行う主回路手段と、前記入出力されるデータを暗号化または解読する暗号処理手段とを有し、前記外部装置との間で暗号化されたデータの入出力が行われることを特徴とする集積回路。

【請求項 2】 外部装置との間でデータの入出力が行われ、該入出力されるデータを処理する集積回路において、該集積回路は、前記集積回路の機能に基づく種々の動作を行う主回路手段と、前記主回路手段から出力されるデータを暗号化する暗号化手段と、前記外部装置から入力される暗号化されたデータを解読する解読手段とからなる暗号処理手段とを有し、前記外部装置との間で暗号化されたデータの入出力が行われることを特徴とする集積回路。

【請求項 3】 前記主回路手段が CPU であり、前記集積回路は 1 チップに形成された 1 チップマイクロコンピュータであることを特徴とする請求項 2 に記載の集積回路。

【発明の詳細な説明】**【0001】**

【産業上の利用分野】 本発明は、外部装置に接続されてデータの入出力を行う集積回路に関し、授受されるデータの複製および集積回路の機能の複製を防止できる集積回路に関する。

【0002】

【従来の技術】 従来、接続される回路すなわち外部装置とデータの入出力を行う集積回路は、入出力されるデータの複製を防止するために、システムを構成する集積回路以外のハードウェアを利用した複製防止データをデータの一部として組み込み、これにより、データの複製を困難にしていた。

【0003】

【発明が解決しようとする課題】 しかし、従来の集積回路に接続された回路とデータの入出力を行う集積回路においては、複製防止データを組み込んだデータを用いる場合であっても、集積回路が実動作しているとき、集積回路に入出力するデータをサンプルすることにより、データの部分的な複製が可能であり、これを防止することはできないという問題があった。

【0004】 本発明は、このような問題を解消し、プログラムまたはデータの複製防止機能を有する集積回路を提供することを目的とする。

【0005】

【課題を解決するための手段】 本発明の集積回路は、上記課題を解決するために、集積回路の機能に基づく種々の動作を行う主回路手段と、入出力されるデータを暗号化または解読する暗号処理手段とを有する。

【0006】

【作用】 本発明によれば、入出力されるデータを暗号化または解読する暗号処理手段を具備しているから、主回路手段から出力されるデータを暗号化して外部装置へ出力するか、または外部装置から入力される暗号化されたデータを解読して主回路手段へ出力することができる。そして、集積回路と外部装置との間で入出力されるデータは暗号化されたデータであるから、入出力されるデータを複製しても、解読手段がなければこのデータを利用することができない。したがって、主回路の機能のみを複製した回路ではこのデータを使用することができない。また、データが暗号化されているため、主回路の複製も困難である。

【0007】

【実施例】 次に図面を用いて本発明の実施例を説明する。図 1 に、本発明による集積回路の一実施例を示す。図 1 は、集積回路と外部回路とが接続された状態を示す。集積回路 1 は主回路 1 1 および暗号化・解読回路 1 2 を備えている。主回路 1 1 は、集積回路 1 の主な機能を実現するものであり、集積回路 1 の機能に基づく種々の動作を行う。主回路 1 1 は、たとえば CPU によって構成される。

【0008】 暗号化・解読回路 1 2 は、データの暗号化および暗号化されたデータの解読の機能を有する回路であり、同図に示すように暗号化回路 1 2 a と解読回路 1 2 b とにより構成されている。暗号化回路 1 2 a は主回路 1 1 から入力されるデータを暗号化して外部回路 2 へ出力し、解読回路 1 2 b は外部回路 2 から入力されるデータを解読して主回路 1 1 へ出力する。

【0009】 暗号化の方式としては種々のものを用いることが可能であるが、本実施例においては U S A スタンダード暗号化方式 (DES) をベースとしたアルゴリズムにより暗号化を行う。

【0010】 DES は、0 と 1 からなる 2 元データに対するブロック暗号であり、2 元データを 6 4 ビットのブロックに分割し、各ブロックについて転置と換字を繰り返すことにより暗号化を行うものである。この場合に転置はあらかじめ固定された変換であるが、換字には 6 4 ビットのキーが使用され、このキーによって換字が制御される。一方、復号すなわち解読においては、暗号化とは逆に換字および転置が繰り返される。

【0011】 暗号化・解読回路 1 2 には外部回路 2 が接続されている。外部回路 2 は集積回路 1 との間でデータを授受する外部装置であり、たとえば集積回路 1 から出力されるデータを記憶する記憶装置、または集積回路 1 によって処理されるデータを読み出す記憶装置である。

なお、図示しないが、データの入出力を制御するインタフェース制御回路たる入出力回路を暗号化・解読回路12に接続し、この入出力回路を通して外部回路2とのデータの授受を行うようにしてもよい。

【0012】この装置によれば、集積回路1が外部回路2にデータを出力する場合、主回路11により処理され出力されたデータは暗号化・解読回路12に入力され、暗号化回路12aにより暗号化される。暗号化回路12aに入力されたデータは前述のような暗号化によって暗号化されたデータに変換される。暗号化されたデータは、外部回路2へ出力される。

【0013】一方、外部回路2から集積回路1へデータが入力される場合には、外部回路2から入力される暗号化されたデータは暗号化・解読回路12の解読回路12bで解読された後、主回路11に供給され所定の処理が行われる。

【0014】このように暗号化・解読回路12により暗号化されたデータが外部装置2へ出力され、また、外部装置2からは暗号化されたデータが入力された暗号化・解読回路12により解読される。したがって、外部装置2との間で入出力されるデータは暗号化されたデータであるから、集積回路1に入出力されるデータを複製しても解読手段を持たない限り、複製したデータを利用することができず、主回路11の機能のみを複製した回路ではこのデータを使用することができない。また、データが暗号化されているため、主回路11の複製も困難である。

【0015】図2には、外部回路2として記憶装置21を接続した場合の例が示されている。記憶装置21は、集積回路1によって処理され、出力されたデータを記憶する記憶装置であり、集積回路1から出力される暗号化されたデータが格納される。この場合には、図1の暗号化・解読回路12の機能は暗号化機能のみで十分であるから、暗号化回路12aに置き換えられている。

【0016】このように接続された装置において、第三者が記憶装置21に格納されたデータを複製した場合にも、複製データを得た者はこのデータを解読する手段を持たない限り、このデータを利用することができない。したがって、集積回路1は複製から保護される。

【0017】図3には、外部回路2として読み出し専用の記憶装置22が使用された場合の例が示されている。この場合には記憶装置22にあらかじめ格納された暗号化されたデータが集積回路1へ読み出され、処理される。この場合には、図1の暗号化・解読回路12の機能は解読機能のみで十分であるから、解読回路12bに置き換えられている。記憶装置22に格納されるデータは主回路11が必要とするデータをあらかじめ暗号化したデータである。この暗号化はたとえば前述のDESによって行われる。図6に示すように、主回路11が必要とする主回路データを供給し（ステップ31）、このデー

タをブロックに分割し（ステップ32）、転置および換字を所定の回数繰り返して暗号化を行い（ステップ33）、暗号化されたデータを得て記憶装置22に格納する（ステップ34）。

【0018】図4には、本発明による集積回路が2個接続された場合の例が示されている。集積回路41は、主回路411および暗号化・解読回路412を有し、暗号化・解読回路412は暗号化回路412aおよび解読回路412bを含んでいる。同様に、集積回路42は主回路421および暗号化・解読回路422を有し、暗号化・解読回路422は暗号化回路422aおよび解読回路422bを含んでいる。暗号化回路412aは解読回路422bに接続され、暗号化回路422aは解読回路412bに接続されている。

【0019】この装置によれば、集積回路41の主回路411から出力されたデータは暗号化回路412aで暗号化され、集積回路42の解読回路422bで解読された後、主回路421へ送られる。また、集積回路42の主回路421から出力されたデータは暗号化回路422aで暗号化され、集積回路41の解読回路412bで解読された後、主回路411へ送られる。

【0020】集積回路41の主回路411と集積回路42の主回路421の主回路としての機能は通常異なるものである。また、集積回路41の行う暗号化と集積回路42の行う暗号化のアルゴリズムは同じものである必要はないが、暗号化回路412aが生成する暗号を解読回路422bが解読でき、かつ、暗号化回路422aが生成する暗号を解読回路412bが解読できるようにされている。集積回路41と集積回路42の暗号化アルゴリズムが異なる場合には、データ複製防止機能はさらに向上する。

【0021】図5には、本発明による集積回路がワンチップマイクロコンピュータ6および入出力用集積回路63として用いられ、これらが互いに接続されるとともに、メモリ64に接続された場合の一例が示されている。ワンチップマイクロコンピュータ6はCPU61、暗号化・解読回路62aおよび暗号化・解読回路62bを有しており、CPU61が図1の主回路11に相当する。入出力用集積回路63は、暗号化・解読回路631および入出力回路632を有し、入出力回路632が図1の主回路11に相当する。

【0022】ワンチップマイクロコンピュータ6の暗号化・解読回路62aは、入出力用集積回路63の暗号化・解読回路631と接続され、暗号化・解読回路62bはメモリ64と接続されている。入出力用集積回路63の入出力回路632は入出力端子65を介して外部装置と接続されている。

【0023】ワンチップマイクロコンピュータ6に接続されたメモリ64には、CPU61のプログラムとデータが暗号化されたデータとして格納されている。メモリ

64から読み出されたプログラムおよびデータは暗号化・解読回路62bにおいて解読され、CPU61に送られる。CPU61はこのプログラムおよびデータにより所定の処理を行う。

【0024】また、CPU61からのデータは暗号化・解読回路62aにおいて暗号化されて入出力用集積回路63の暗号化・解読回路631に送られ、暗号化・解読回路631で解読された後、入出力回路632に送られる。そして入出力回路632で入出力処理を行われた後、入出力端子65を通して外部装置へ出力される。逆に、外部装置から入出力端子65を通して入力されたデータは、入出力回路632で入出力処理を行われた後、暗号化・解読回路631に送られて暗号化され、ワンチップマイクロコンピュータ6の暗号化・解読回路62aへ出力される。データは暗号化・解読回路62aで解読され、CPU61に送られる。CPU61で処理されたデータは暗号化・解読回路62bにおいて暗号化され、メモリ64に記憶される。

【0025】本装置においても、前述のような暗号化アルゴリズムによって暗号化されたデータがワンチップマイクロコンピュータ6、入出力用集積回路63およびメモリ64の間で入出力される。

【0026】一般に乱数を用いた暗号化や暗号化鍵によるビット反転とビット入れ換え操作を多段数行う暗号化では、暗号化アルゴリズムを知らずに暗号化されたデータやプログラムを解読することは、非常に困難である。また、集積回路のマスクパターンから暗号化アルゴリズムを解析するか、あるいは、CPU61と暗号化・解読回路62a、62bの間の信号を解析することが非常に困難であることは言うまでもない。

【0027】図5の実施例においては、メモリ64に格納されたデータまたはプログラムを複製しても、このデータを解読しないかぎり利用できないため、CPU61のデータまたはプログラムを保護することができる。また、入出力用集積回路63に対するコマンドやデータが暗号化されていることにより、入出力集積回路63のコマンド体系やデータ形式が保護されるため、入出力集積回路63の複製を防止できる。

【0028】

【発明の効果】以上説明したように本発明によれば、集

* 積回路には暗号化されたデータが入出力されるから、入出力されるデータを複製しても、主回路の機能のみを複製した回路ではこのデータを使用することができない。暗号化されたデータを解読するには暗号化アルゴリズムを調査しデータを解読するか、または、集積回路の内部で主回路と暗号化・解読回路の間の信号を直接サンプリングしなければならないため、データの複製は非常に困難である。また、データを暗号化しているため主回路の複製も困難であるから、回路を複製から有効に保護することができる。

【図面の簡単な説明】

【図1】本発明による集積回路の一実施例を示すブロック図である。

【図2】本発明による集積回路を記憶装置に接続した実施例を示すブロック図である。

【図3】本発明による集積回路を読み出し専用記憶装置に接続した実施例を示すブロック図である。

【図4】本発明による集積回路を2個接続した実施例を示すブロック図である。

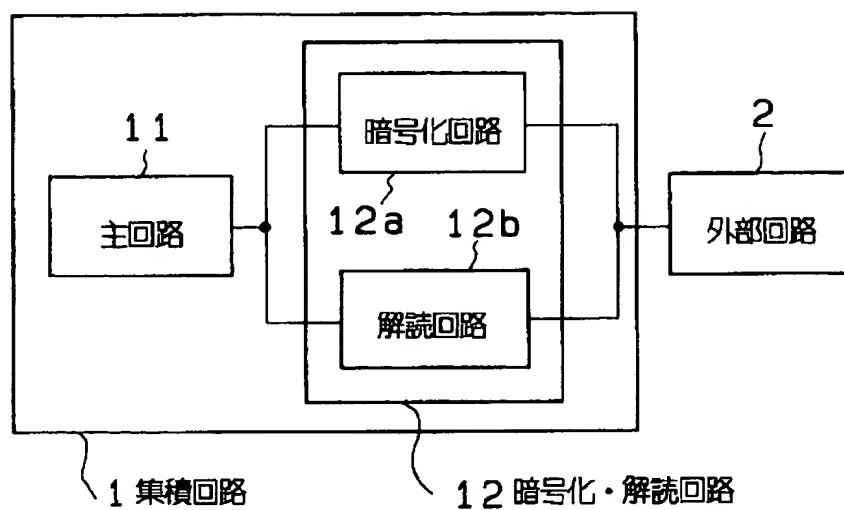
【図5】本発明による集積回路をワンチップマイクロコンピュータおよび入出力用集積回路として用いた実施例を示すブロック図である。

【図6】暗号化データを作成する手順を示すフロー図である。

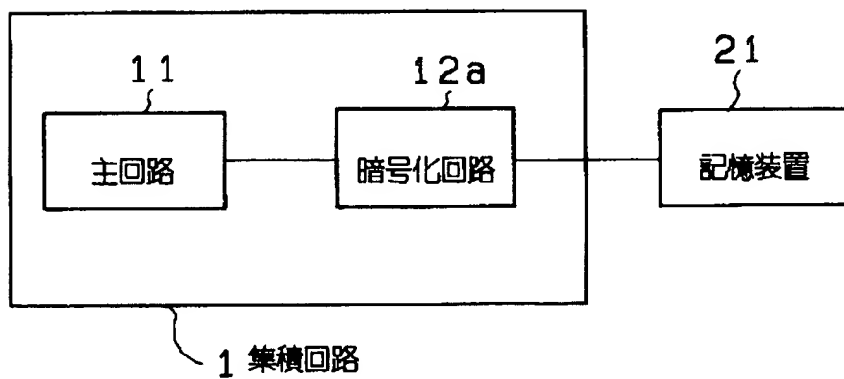
【符号の説明】

- 1 集積回路
- 2 外部回路
- 6 ワンチップマイクロコンピュータ
- 12 暗号化・解読回路
- 21 記憶装置
- 22 記憶装置
- 41 集積回路
- 42 集積回路
- 61 CPU
- 62a 暗号化・解読回路
- 62b 暗号化・解読回路
- 63 入出力集積回路
- 64 メモリ
- 65 入出力端子

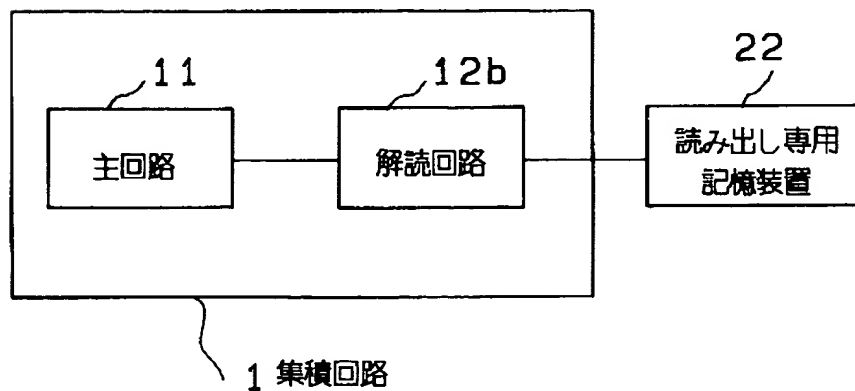
【図1】



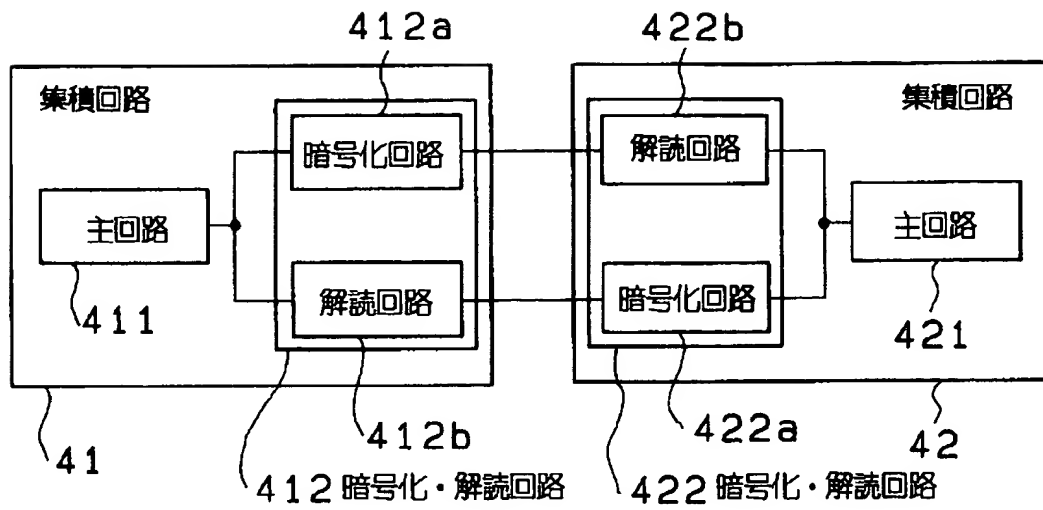
【図2】



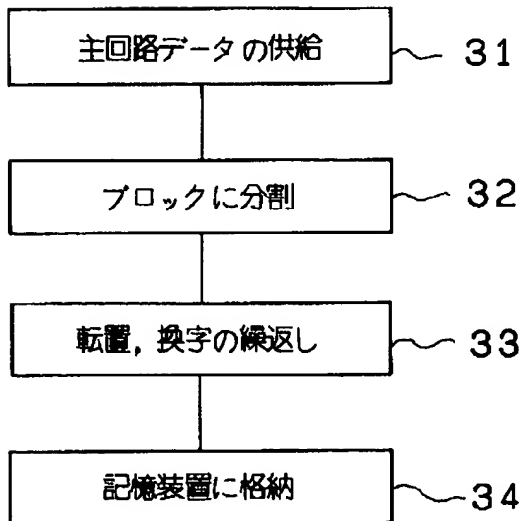
【図3】



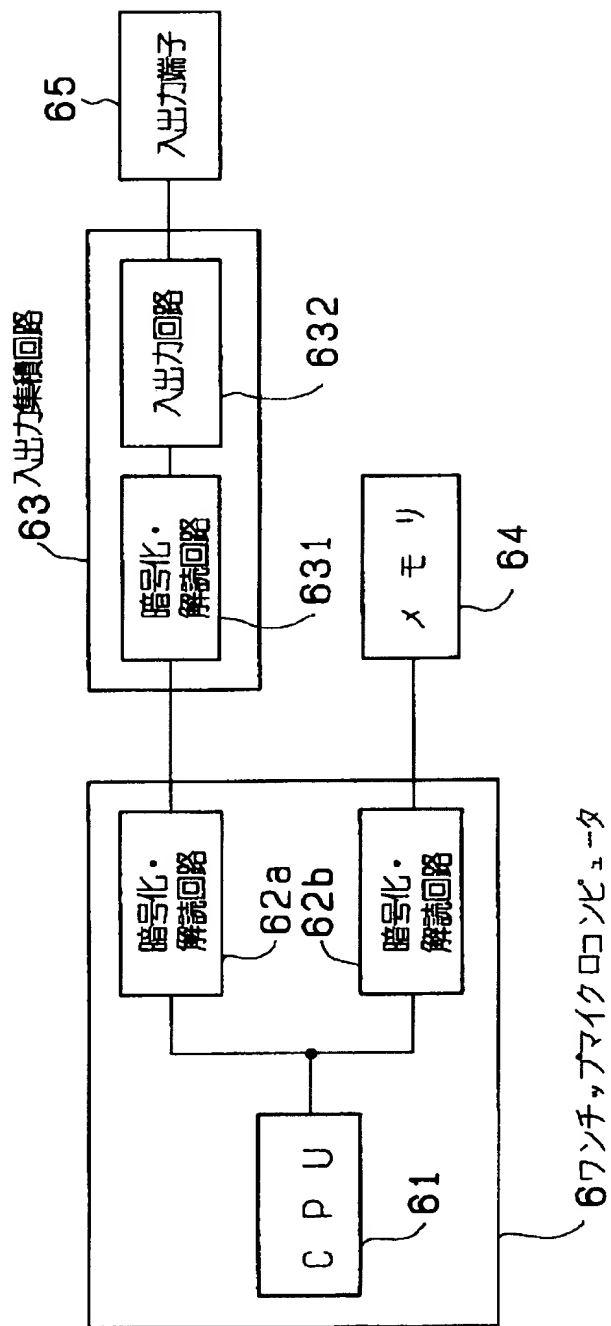
【図4】



【図6】



【図 5】



⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑬ 公開特許公報(A)

昭64-41947

⑤ Int. Cl.⁴
G 06 F 12/14

識別記号
3 2 0

庁内整理番号
B-7737-5B

④ 公開 昭和64年(1989)2月14日

審査請求 未請求 発明の数 1 (全11頁)

⑫ 発明の名称 半導体集積回路

② 特 願 昭62-197582

③ 出 願 昭62(1987)8月7日

⑦ 発 明 者 和 田 浩 史 東京都青梅市今井2326番地 株式会社日立製作所デバイス開発センタ内

⑧ 発 明 者 長 谷 川 直 宏 埼玉県入間郡毛呂山町大字旭台15番地 日立東部セミコンダクタ株式会社内

⑨ 出 願 人 株式会社日立製作所 東京都千代田区神田駿河台4丁目6番地

⑨ 出 願 人 日立東部セミコンダクタ株式会社 埼玉県入間郡毛呂山町大字旭台15番地

④ 代 理 人 弁理士 玉村 静世

明 細 書

1. 発明の名称

半導体集積回路

2. 特許請求の範囲

1. 機密保持すべき情報を格納する記憶領域を含んで1つの半導体基板に形成された半導体集積回路であって、外部との情報のやりとりに際してその情報を直接又はその情報のやりとりのための制御情報を、暗号化し又は復号化するための情報変換手段を内蔵して成るものであることを特徴とする半導体集積回路。

2. 上記情報変換手段は、キーワード情報により、暗号化又は復号化される情報を可変とする暗号化又は復号化のアルゴリズムを有するものであることを特徴とする特許請求の範囲第1項記載の半導体集積回路。

3. 上記記憶領域を含んで1つの半導体基板に形成された半導体集積回路は、半導体記憶装置であって、その記憶領域には暗号化された情報が保持され、その保持情報を復号化して外部に与

えるようにされて成るものであることを特徴とする特許請求の範囲第2項記載の半導体集積回路。

4. 上記記憶領域の一部は、上記キーワード情報格納領域とされ、その領域に格納されたキーワード情報が出力情報の復号化アルゴリズムを決定するようにされて成るものであることを特徴とする特許請求の範囲第3項記載の半導体集積回路。

5. 上記記憶領域を含んで1つの半導体基板に形成された半導体集積回路は、少なくとも内部バスに結合された記憶領域と中央処理装置を機能ブロックとして含むと共に、前記内部バスの情報は、テストモード設定時に出力回路を介して外部に開放され得るマイクロコンピュータユニットであり、上記データ変換手段は、出力バッファ回路の出力情報を暗号化するようにされて成るものであることを特徴とする特許請求の範囲第1項又は第2項記載の半導体集積回路。

6. 上記記憶領域を含んで1つの半導体基板に形

成された半導体集積回路は、少なくとも内部バスに結合された記憶領域と中央処理装置を機能ブロックとして含むと共に、前記内部バスの情報は、テストモード設定時に出力回路を介して全て外部に開放され得るマイクロコンピュータユニットであり、上記データ変換手段は、テストモード設定情報を復号化して上記出力回路の出力制御を行うようにされて成るものであることを特徴とする特許請求の範囲第1項又は第2項記載の半導体集積回路。

3. 発明の詳細な説明

(産業上の利用分野)

本発明は半導体集積回路さらにはそれに含まれる情報の機密保持のための技術に関し、例えばメモリに含まれるデータやシングルチップマイクロコンピュータに含まれるソフトウェアプログラムなどの機密保持に適用して有効な技術に関するものである。

(従来技術)

本発明者らは、LSIにおける機密保護、例え

相互に結合されているが、システム動作時にはその内部バスの情報は直接外部に開放されず、内蔵される入出力回路を介して外部とインタフェースされる。しかしながら、斯る構成では、動作中に発生した不良箇所が外部から判断できないためにLSIのテストモード時における不良解析が困難になることがある。そこで、CPUとメモリなどを結合する内部バスが外部に開放されないようなLSIにおいて、テストモードの設定によって内部バスを外部から自由にアクセス可能とするようなバッファ回路を設けてテスト効率の向上を図ることが行われている。

(発明が解決しようとする問題点)

複数のLSIチップによってシステム構成される場合に上記したパッケージングによる機密保持方式は経済的に高価であり、安価な民生機器に利用することができない場合が多い。

また、シングルチップマイクロコンピュータのようなシステムLSIの場合、当該LSIに含まれる各機能ブロックが外部から自由にアクセス可

ば、メモリに格納されているソフトウェアプログラムやその他のデータの機密保護について検討した。

それによれば、ある特定のシステムが1つのLSIにシステムオンチップ化されず複数のLSIによって構成される場合、当該システムを構成する複数のLSIを1かたまりとしてパッケージングするケースが無理に開かれようとするとき、それに連動して機密保持すべきデータが破壊されるようなセキュリティ方式を採用することができる。

ところで、今日、LSIの高集積化に伴ってLSIへのシステムオンチップ化が促進され、例えば、中央処理装置もしくはCPU(セントラル・プロセッシング・ユニット)を中心に、プログラムメモリ、データメモリ、入出力回路、及びその他の周辺回路を1つの半導体基板上に搭載して成る所謂シングルチップマイクロコンピュータが提供されている。

このようなシングルチップマイクロコンピュータに含まれる各機能ブロックは内部バスによって

能にされると、そのLSIに含まれる機密保持すべきソフトウェアプログラムやデータが不正なアクセスによつて簡単に盗まれるという問題点が発明者らによって明らかにされた。斯る不正なアクセスは、LSIにオンチップ化されたシステムに関するだけでなく、メモリなど単体の各種LSIに対しても考慮されるべき事柄である。

本発明の目的は、保有する情報を自らが機密保持する機能を有する半導体集積回路を提供することにある。

本発明の前記ならびにそのほかの目的と新規な特徴は本明細書の記述及び添付図面から明らかになるであろう。

(問題点を解決するための手段)

本願において開示される発明のうち代表的なものの概要を簡単に説明すれば下記の通りである。

すなわち、外部との情報のやりとりを際してその情報を直接又はその情報のやりとりのための制御情報を暗号化し又は復号化するための情報変換手段を、機密保持すべき情報を格納する記憶領域

を含んで1つの半導体基板に形成された半導体集積回路に含めたものである。例えば、少なくとも内部バスに結合されたプログラム記憶領域と中央処理装置を機能ブロックとして含むと共に、前記内部バスの情報は、テストモード設定時に出力バッファ回路を介して全て外部に開放され得るマイクロコンピュータにおいて、上記情報変換手段は、キーワード情報に従った暗号化アルゴリズムより、出力バッファ回路の出力を暗号文とする暗号化器、又はキーワード情報に従った復号化アルゴリズムにより、暗号化されているテストモード設定コードを復号化して出力バッファ回路の出力動作を制御する復号化器とされる。

〔作用〕

上記した手段によれば、情報変換手段に予め定められたキーワード情報を用いなければ、テストモードを設定することができず、あるいは、テストモードを設定しても正規のデータを出力バッファ回路から読み出すことができず、それによって、機密保持すべきソフトウェアプログラムなどに対

ド・プログラマブル・リード・オンリ・メモリ) 5、入出力回路6、その他の周辺回路7が内部バス8に結合されて含まれている。

上記EEPROM5は、夫々図示しないメモリアレイ、アドレスデコーダ、データ入出力回路、書き込み回路、EEPROM5全体の制御を司るシーケンス制御回路などを含み、データの半永久的な記憶に利用される。上記RAM3は主としてデータの一時記憶、或いはCPU2の作業領域とされる。上記CPU3は、例えば、夫々図示しない汎用レジスタ、プログラムカウンタ、コンディションコードレジスタ、算術論理演算器などを含み、主として前記ROM4から順次命令を読み込んで所定の処理動作を実行する。上記ROM4は、特に制限されないが、EPROM(エレクトリカル・プログラマブル・リード・オンリ・メモリ)やマスクROMによって構成され、各種情報処理のためのソフトウェアプログラムが格納されている。

上記入出力回路6と外部とのインタフェースは、

する不正アクセスの防止を当該LSI自体の機能によって達成する。

〔実施例1〕

第1図は本発明の第1実施例に係るシングルチップマイクロコンピュータを示すブロック図である。

第1実施例は、シングルチップマイクロコンピュータ1が保有する所定のデータをシステム動作時に外部に出力する場合における当該出力データの機密保持を行うための構成とされる。例えば、LSI相互間における機密情報の伝達を行うような場合に適用される。

第1図に示されるシングルチップマイクロコンピュータは、公知の半導体集積回路製造技術によってシリコン単結晶のような1つの半導体基板に形成されている。このシングルチップマイクロコンピュータ1は、特に制限されないが、CPU2を中心に、RAM(ランダム・アクセス・メモリ)3、ROM(リード・オンリ・メモリ)4、EEPROM(エレクトリカル・イレーザブル・アン

外部に出力すべきデータを選択的に暗号化して外部に供給する暗号化器9と、外部から供給されるデータを選択的に復号化して内部に与える復号化器10を介して行われる。暗号化器9及び復号化器10における、暗号化・復号化アルゴリズムは、複数ビットから成る所定のキーワード情報KEYに従って決定される。即ち、キーワード情報KEYに対応して、暗号化及び復号化のアルゴリズムが可変とされる。したがって、予め定められた所定のキーワード情報KEYが暗号化器9や復号化器10に与えられない限り、平文と暗号文は実質的に有意な相関を有しない。暗号化器9及び復号化器10における暗号化動作及び復号化動作は、リセット信号RESETにより選択的に解除可能とされる。

ここで、CPU2は、特に制限されないが、ROM4に格納されている命令を順次読み込みながら所定の処理動作を実行するが、そのデータ処理動作の過程において機密保持すべきデータが生じた場合には、そのデータを、機密保持すべきデー

タのための専用の記憶領域に格納する。所る機密保持すべきデータ専用の記憶領域は、予めRAM3やEEPROM5などに設定され、そのアドレスはCPU2が管理する。CPU2は、機密保持すべきデータを外部に転送するとき、及び、外部から機密保持すべきデータの転送を受けるとき、前記リセット信号RESETをディスイネーブルレベルにして、暗号化器9及び復号化器10を暗号化動作及び復号化動作可能な状態に制御する。

尚、機密保持すべきデータに関しては、内部において機密保持すべきデータであることを意味する制御ビットを当該データに含め、そのデータをRAM3やEEPROM5に保存するようにしてもよい。

第1図において、キーワード情報KEYは外部から与えられるようになっているが、キーワード情報KEYの伝達途上における安全性確保の点から、当該キーワード情報KEYをEEPROM5などの所定エリアに格納しておき、CPU2が上記リセット信号RESETをディスイネーブルレ

そのままの順序で供給される。セレクト12における各ビットの入力端子Hには、入力レジスタ11の各出力ビットデータがランダムな順番にされて供給される。セレクト12の各ビットにおける入力端子H又はLからの入力選択は、各選択端子Sに供給される選択信号のレベルによって決定され、例えば、選択端子Sにハイレベルのビットデータが与えられるときには入力端子Hからの入力を選択し、選択端子Sにロウレベルのビットデータが与えられるときには入力端子Lからの入力を選択する。セレクト12の各ビットにおける選択信号は、特に制限されないが、前記キーワード情報KEYが供給されるシリアルイン・パラレルアウト形式のシフトレジスタ14における各パラレル出力データとされる。

シフトレジスタ14がリセット信号RESETによってリセットされると、そのパラレル出力データは全ビットがロウレベルとされ、それによって、セレクト12は実質的に転置処理もしくはデータスクランブル処理を行わず、出力データD

outに制御するタイミングに呼応して、当該キーワード情報KEYをEEPROM5などから暗号化器9及び復号化器10に与えるようにしてもよい。

第2図は上記暗号化器9の一例を示すブロック図である。この暗号化器9は、内部から平文Dinがパラレルに供給される入力レジスタ11を有し、入力レジスタ11の各出力ビットは、セレクト12によって所定の転置処理もしくはスクランブル処理可能とされ、セレクト12の出力データは、出力レジスタ13を介して外部にパラレル出力される。尚、入力レジスタ11及び出力レジスタ13は、クロック信号CLKに同期するタイミングでその入出力動作が行われる。

上記入力レジスタ11、セレクト12、及び出力レジスタ13は相互に同一のビット構成とされ、セレクト12の各ビットは、入力端子H及びLを有する。セレクト12における各ビットの入力端子Lにはセレクト12と1対1対応でビット対応される入力レジスタ11の各出力ビットデータが

utは平文Dinと同一とされる。シフトレジスタ14がリセットされない状態にあっては、セレクト12は、キーワード情報KEYに応じた暗号化アルゴリズムに従って平文Dinの各ビットを転置もしくはスクランブルし、それによって、平文Dinに対応する出力データDoutは暗号文とされる。

復号化器10は、特に制限されないが、第2図に示される暗号化器9と同様に構成することができる。その場合に復号化器10は、暗号化器9における暗号文生成時に用いられたキーワード情報KEYにより、当該暗号文を平文に変換し得る復号化アルゴリズムを有するようにセレクトの入力端子と入力レジスタの出力端子が結合されることになる。

上記実施例1によれば以下の作用効果を得るものである。

(1) シングルチップマイクロコンピュータ1は、それが保有する情報のうち、機密保持すべきデータをシステム動作時に外部に出力する場合に、選

択的に当該データを平文から暗号文に変換することができることにより、情報伝達に際して所望の情報をシングルチップマイクロコンピュータ1自体の機能によつて機密保持することができる。

(2) キーワード情報KEYをEEPROM5などのメモリの所定エリアに予め格納しておき、CPU2が必要に応じて当該キーワード情報KEYを所定の記憶領域から暗号化器9や復号化器10に与えるようにすることにより、キーワード情報KEYの伝達途上における安全性をシングルチップマイクロコンピュータ自体の機能によつて確保することができ、シングルチップマイクロコンピュータ1が備える機密保持機能を一層完全化することができる。

(3) さらにこのような機密保持機能付きのLSIによつてシステムを構築すると、システム内での機密情報の転送は暗号化されて行われることにより完全化される。

【実施例 2】

第3図は本発明の第2実施例に係るシングルチ

ップマイクロコンピュータ20、30のシステム動作時において、その内部バス8の情報はCPU2によつてアクセスされる入出力回路7を介して外部とインタフェースされる。したがって、ROM4が保有するソフトウェアプログラム、さらにはRAM4やEEPROM5が保有して専ら内部処理だけに利用されるようなデータは外部に直接的に開放されない。そこで、動作中に発生した不良個所を外部から直接判断することができるようにしてテスト時における不良解析の容易化を図るため、テストモードの設定によつて内部バスを外部からアクセス可能とするテスト用入出力回路21、31が設けられている。

第3図に示される第2実施例において、テスト用入出力回路21を介する不正アクセスの阻止は、それに含まれるトライステイト出力バッファ回路22の出力情報を暗号化する暗号化器23によつて達制する。即ち、テスト用入出力回路21には、外部から内部バス8に情報を直接供給可能なトラ

ップマイクロコンピュータを示すブロック図、第4図は本発明の第3実施例に係るシングルチップマイクロコンピュータを示すブロック図である。

第2及び第3実施例は、シングルチップマイクロコンピュータにテストモードが設定される場合において、外部に開放可能とされる内部バスを介する不正なアクセスの阻止に適用される。

第3図に示されるシングルチップマイクロコンピュータ20及び第4図に示されるシングルチップマイクロコンピュータ30は、上記実施例同様、1つの半導体基板に形成され、夫々に含まれるCPU2、RAM3、ROM4、EEPROM5、入出力回路6、及びその他周辺回路7は、第1図に示されるものと同様の機能ブロックであり、各機能ブロックは内部バス8によつて相互に結合されている。第3図及び第4図に示される入出力回路7には、第1実施例で説明した暗号化器9及び復号化器10が図示されていないが、シングルチップマイクロコンピュータ20、30にそれらを含めることは自由である。

イスティット入力バッファ回路24と内部バス8の情報を外部に与えるためのトライステイト出力バッファ回路22とを有し、トライステイト出力バッファ回路22の出力端子は暗号化器23を介して外部に接続されている。

トライステイト入力バッファ回路24及びトライステイト出力バッファ回路22の制御端子にはテストモード設定信号Btestが供給される。テストモード設定信号Btestは、特に制限されないが、そのハイレベルによつてテストモードを指示する。テストモード設定信号Btestがロウレベルにされると、トライステイト入力バッファ回路24及びトライステイト出力バッファ回路22は夫々高出力インピーダンス状態に制御され、また、テストモード設定信号Btestがハイレベルにされると、トライステイト入力バッファ回路24及びトライステイト出力バッファ回路22は夫々入力信号レベルに応じた出力信号を出力可能な状態に制御される。

上記暗号化器23は、第1実施例同様、複数

ビットから成る所定のキーワード情報KEYに応じてその暗号化アルゴリズムが決定される。したがって、予め定められた所定のキーワード情報KEYが暗号化器23に与えられない限り、平文としての内部バス8の情報と暗号文として外部に与えられる情報との間における有意味の相関を知ることはできない。暗号化器23の具体的回路構成は第2図のようにすることができるが、本実施例の場合には、暗号化器23の動作を選択する必要はないから上記実施例のようなリセット機能は省略することができる。尚、テストモードを設定してマイクロコンピュータを診断するとき、暗号化器23から出力される暗号情報は、テストで復号化されて診断に供されることになる。

第4図に示される第3実施例において、テスト用入出力回路31を介する不正アクセスの阻止は、複数ビットのデータによって構成されるテストモード設定コードCtestを復号化してトライステイト出力バッファ回路32の出力制御を行う復号化器33によって連制する。即ち、テスト用入

出力回路31には、外部から内部バス8に情報を与えるためのトライステイト入力バッファ回路34と内部バス8の情報を外部に与えるためのトライステイト出力バッファ回路32とを有する。トライステイト入力バッファ回路34及びトライステイト出力バッファ回路32の制御端子には復号化器33の出力端子が結合される。この復号化器33は、その入力端子から供給されるテストモード設定コードCtestを、所定ビット数のキーワード情報KEYに応じた復号化アルゴリズムに従って復号化して出力する。即ち、本実施例においては、正規のテストモード設定コードCtest及びキーワード情報KEYが復号化器33に供給されて初めて当該シングルチップマイクロコンピュータ30にテストモードを設定することができる。言い換えるなら、テストモード設定コードCtest自体が所定の暗号化アルゴリズムに従って暗号化されているから、正規のテストモード設定コードCtestはもとよりそれを得るための暗号化アルゴリズムに対応される正規のキー

ワード情報KEYを知らなければ、当該シングルチップマイクロコンピュータ30にテストモードを設定することができない。

第3図及び第4図において、キーワード情報KEYは外部から与えられるようになっているが、キーワード情報KEYの伝達途上における安全性確保の点から、当該キーワード情報KEYをEEPROM5などのメモリの所定エリアに予め格納しておき、テストモードの設定に呼応してCPU2が当該キーワード情報KEYをEEPROM5などから暗号化器23又は復号化器33に与えるようにしてもよい。

上記実施例2によれば以下の作用効果を得るものである。

(1) 第2実施例によれば、テストモードが設定されても、テスト用入出力回路21における暗号化器23に正規のキーワード情報が供給されなければ、平文としての内部バス8の情報と外部に供給される暗号文との間の相関を知ることはできない。また、第3実施例によれば、テストモード設

定コードCtest自体が所定の暗号化アルゴリズムに従って暗号化されているから、正規のテストモード設定コードCtestはもとよりそれを得るための暗号化アルゴリズムに対応される正規のキーワード情報KEYが復号化器33に与えられなければ、当該シングルチップマイクロコンピュータ30にテストモードを設定することができない。したがって、テストモードの設定によって内部バス8を外部に開放し得る機能を不正に利用して、システム動作時には外部に開放されないソフトウェアプログラムや所定のデータの機密が失われることを、シングルチップマイクロコンピュータ20、30自体の機能によつて防止することができる。

(2) 第2実施例及び第3実施例のプロテクト機構を共に採用することにより、必要な情報の機密保持機能を一層向上させることができる。

(3) キーワード情報KEYをEEPROM5などの所定記憶エリアに予め格納しておき、テストモードの設定に呼応してCPU2が当該キーワ

ード情報KEYをEEPROM5などから暗号化器23又は復号化器33に与えるようにすることにより、キーワード情報KEYの伝達途上における安全性をシングルチップマイクロコンピュータ自体の機能によって確保することができ、シングルチップマイクロコンピュータ20,30が備える機密保持機能を一層完全化することができる。

【実施例3】

第5図は本発明の第4実施例に係る半導体記憶装置を示すブロック図、第6図は本発明の第5実施例に係る半導体記憶装置を示すブロック図である。

第4実施例及び第5実施例は、不正なアクセスを阻止する機能を半導体記憶装置自体に適用したものであり、機密保持すべきデータを暗号化して保持すると共に、暗号化されたデータをキーワード情報に従って復号化処理して読み出すようにしたものである。

第5図に示される半導体記憶装置40は、特に制限されないが、EEPROM、EPROM、ス

RDATAとして出力される。

したがって、データ書き込み時のキーワード情報KEYを知らなければ当該半導体記憶装置40からは有意のデータを読み出すことができないことにより、格納データの機密保持を達成する。

尚、本実施例はマスクROMのような固定ROMにも適用することができるが、その場合にメモリセルが保持するデータは予め暗号化されたデータとされ、それに従って暗号化器41は不要とされる。

第6図に示される半導体記憶装置50は、特に制限されないが、EEPROMやEPROMなどの書き込み可能な不揮発性メモリを主体とし、外部から供給されるデータを暗号化して内部に取り込む暗号化器51と、暗号化されて内部に保持されているデータを復号化して外部に与える復号化器52を備える。暗号化器51は第1実施例で説明したものと同様にリセット機能を有し、外部端子から供給されるリセット信号RESETによってリセットされた場合にはその暗号化機能は実質

タティックRAM、ダイナミックRAM、不揮発性RAMなどの書き換え可能なメモリを主体とし、外部から供給されるデータを暗号化して内部に取り込む暗号化器41と、暗号化されて内部に保持されているデータを復号化して外部に与える復号化器42を備える。暗号化器41及び復号化器42は第1実施例で説明したものと同様に外部から供給されるキーワード情報KEYに従った暗号化及び復号化アルゴリズムを有するように構成される。

この半導体記憶装置40において、外部から供給される平文としての書き込みデータWDATAはキーワード情報に従った暗号化アルゴリズムで暗号文に変換されて、外部アドレス信号ADDRに応ずる所定の図示しないメモリセルに格納される。メモリ・リード・アクセスにおいて、所定のメモリセルから読み出される暗号文としてのデータは、データ書き込み時と同じキーワード情報KEYが復号化器42に供給されて初めて意味のある平文データに逆変換されて外部にリードデータ

的に停止されて、外部から供給されるデータをそのままの状態でも内部に与える。

上記暗号化器51及び復号化器52はいままで説明と同様にキーワード情報KEYに従った暗号化及び復号化アルゴリズムを有するように構成されるが、そのキーワード情報KEYは半導体記憶装置50におけるメモリセルアレイ54の所定領域(キーワード情報格納領域)Ekeyに保持される。この所定領域Ekeyに対するキーワード情報KEYの書き込みはメモリ・ライト・アクセスを介して任意に行うことができるが、その場合に暗号化器51はリセット状態にされる。キーワード情報格納領域Ekeyに任意に書き込まれたキーワード情報KEYは、特に制限されないが、チップ選択状態に呼応して暗号化器51及び復号化器52に供給される。この制御は半導体記憶装置50全体の制御を司る図示しないシーケンス制御回路が行う。

この半導体記憶装置50は、ユーザによって予め任意のキーワード情報KEYが所定領域Ekey

メモリに書き込み設定される。この状態で、外部から供給される平文としての書き込みデータWDATAはキーワード情報KEYに従った暗号化アルゴリズムで暗号文に変換されて、外部アドレス信号ADDRに应ずる所定の図示しない不揮発性メモリセルに格納される。メモリ・リード・アクセスにおいて、所定のメモリセルから読み出される暗号文としてのデータは、データ書き込み時と同じキーワード情報KEYが復号化装置52に供給されて初めて意味のある平文データに逆変換されて外部にリードデータRDATAとして出力される。

本実施例の半導体記憶装置50において、キーワード情報KEYは記憶装置自体に保持されているから、前記第3実施例と比較すると、キーワード情報の伝達途上における安全性の確保を外部で特別に考慮することなく、格納データの機密保持を達成する。

上記実施例3によれば以下の作用効果を得るものである。

(1) 機密保持すべきデータを暗号化して保持す

シングルチップマイクロコンピュータのようなLSIにおいてテストモードが設定される際のセキュリティ、さらには半導体記憶装置自体のセキュリティとして類別して説明したが、上記各セキュリティ機能を適宜組合わせて1つのLSIに付加してもよい。

また、EEPROMやEPROMなどのメモリセルにキーワード情報を設定すると、チップ外觀からはそのメモリセルの記憶状態は判別不可能とされるから、暗号化回路や復号化回路自体を、キーワード情報設定用の不揮発性メモリセルを含んで回路構成或いはレイアウト構成することによって、さらにLSIのセキュリティを向上させることができる。

また、上記各実施例では、暗号化及び復号化に同一のキーワード情報を用いる慣用暗号化方式について説明したが、公開キー暗号方式のようにキーワード情報を暗号化と復号化とで相違させるようなアルゴリズムをも適用することができる。更に暗号化及び復号化のアルゴリズムは、キーワ

ードと共に、暗号化されたデータはキーワード情報KEYに従って復号化処理されて読み出されることにより、不正なアクセスを阻止する機能を半導体記憶装置自体の機能によって達成することができる。

(2) キーワード情報KEYがメモリセルアレイにおける所定領域などの半導体記憶装置自体に保持されることにより、キーワード情報の伝達途上における安全性の確保を外部で特別に考慮することなく、格納データの機密保持を達成することにより、半導体記憶装置自体が持つ不正アクセス阻止機能の信頼性を高めることができる。

以上本発明者によってなされた発明を実施例に基づいて具体的に説明したが、本発明はそれに限定されず、その要旨を逸脱しない範囲において種々変更可能であることは言うまでもない。

例えば上記実施例ではLSIに付加したセキュリティ機能を、シングルチップマイクロコンピュータのようなLSIにおける通常のシステム動作時のデータ入出力に際してのセキュリティ、

ード情報を利用するものに限定されない。さらに、暗号化及び復号化のアルゴリズムに関しては、上記各実施例で説明した専用のハードウェアで決定される構成に限定されず、マイクロプロセッサなどを介してソフトウェア的に暗号化及び復号化のアルゴリズムを実現するようにしてもよい。

以上の説明では主として本発明者によってなされた発明をその背景となったシングルチップマイクロコンピュータ及び半導体記憶装置に適用した場合について説明したが、本発明はそれに限定されるものではなく、その他のシステムオンチップLSIなど種々の半導体集積回路に適用することができる。本発明は、少なくとも、機密保持すべき情報を格納する記憶領域を含んで1つの半導体基板に形成された条件のものに適用することができる。

〔発明の効果〕

本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば下記の通りである。

すなわち、外部との情報のやりとりに際してその情報を直接又はその情報のやりとりのための制御情報を暗号化し又は復号化するための情報変換手段を、機密保持すべき情報を格納する記憶領域を含んで1つの半導体基板に形成された半導体集積回路に含めることにより、シングルチップマイクロコンピュータのようなシステムオンチップLSIにおけるシステム動作時のデータ入出力に際して、また、斯るシステムオンチップLSIにおける内部バスを外部に開放するためのテストモード設定に際して、さらには半導体記憶装置に対するリード・アクセスに際して、機密保持すべきソフトウェアプログラムやデータに対する不正アクセスの防止を当該LSI自体の機能によって達成することができる。

4. 図面の簡単な説明

第1図は本発明の第1実施例に係るシングルチップマイクロコンピュータを示すブロック図、

第2図は暗号化器の一例を示すブロック図、

第3図は本発明の第2実施例に係るシングルチ

ップマイクロコンピュータを示すブロック図、

第4図は本発明の第3実施例に係るシングルチップマイクロコンピュータを示すブロック図、

第5図は本発明の第4実施例に係る半導体記憶装置を示すブロック図、

第6図は本発明の第5実施例に係る半導体記憶装置を示すブロック図である。

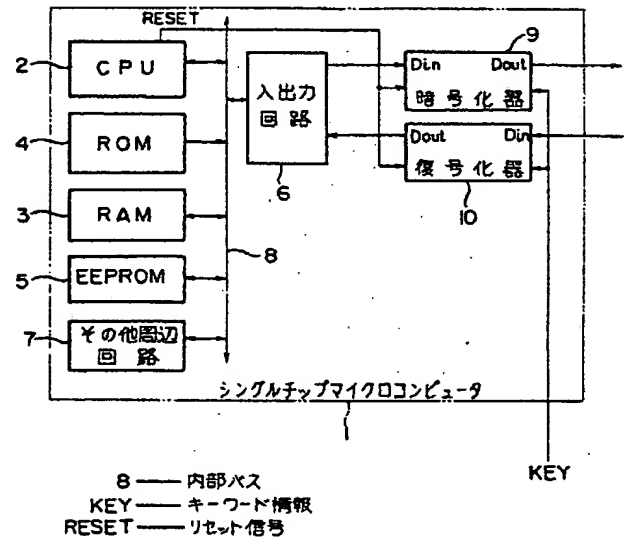
1…シングルチップマイクロコンピュータ、2…CPU、3…RAM、4…ROM、5…EEPROM、6…入出力回路、8…内部バス、9…暗号化器、10…復号化器、KEY…キーワード情報、RESET…リセット信号、11…入力レジスタ、12…セレクタ、13…出力レジスタ、14…シフトレジスタ、20…シングルチップマイクロコンピュータ、21…テスト用入出力回路、22…出力バッファ回路、23…暗号化器、Reset…テストモード設定信号、30…シングルチップマイクロコンピュータ、31…テスト用入出力回路、32…出力バッファ回路、33…復号化器、Ctest…テストモード設定コード、4

0…半導体記憶装置、41…暗号化器、42…復号化器、50…半導体記憶装置、51…暗号化器、52…復号化器、53…メモリセルアレイ、Key…キーワード情報格納領域。

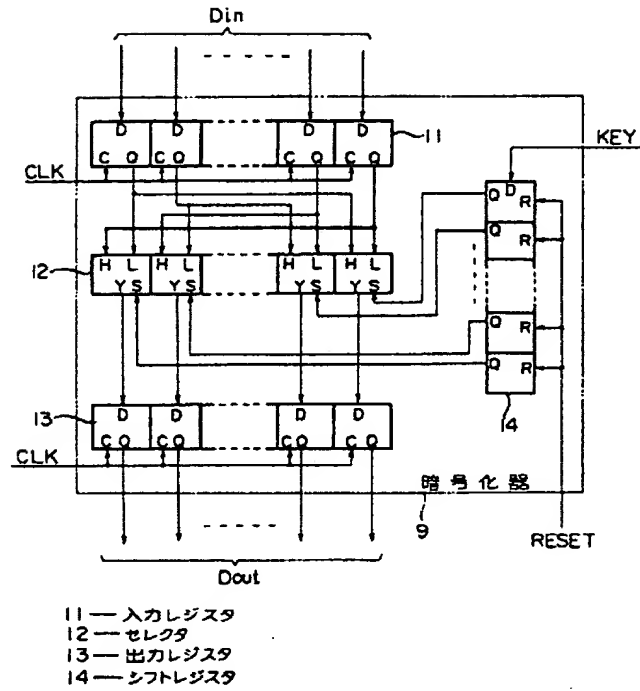
代理人 弁理士 五 村 節 世



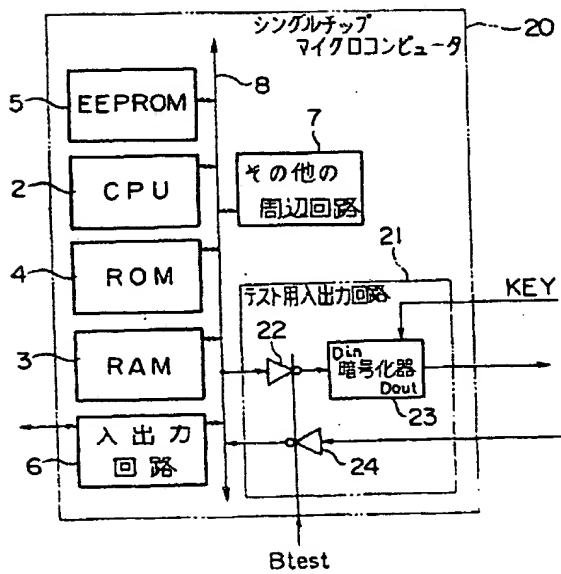
第1図



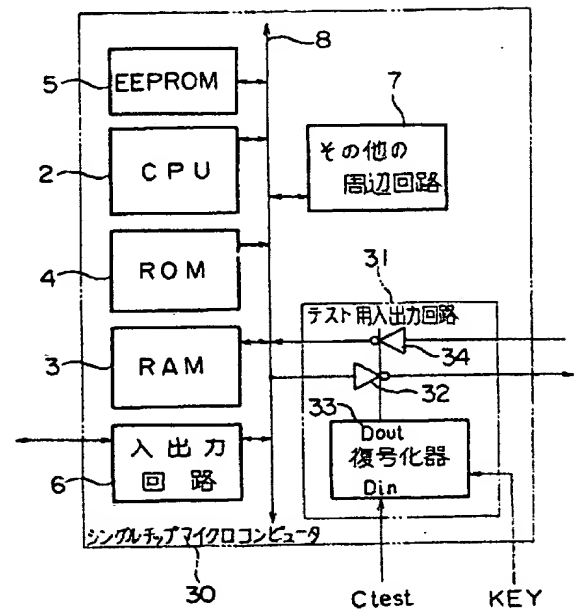
第 2 図



第 3 図

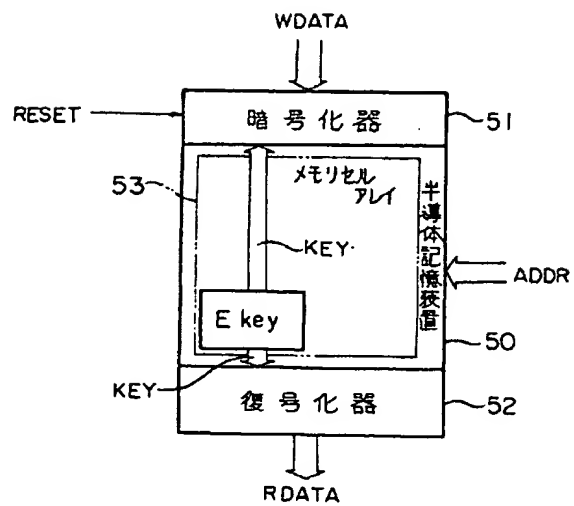
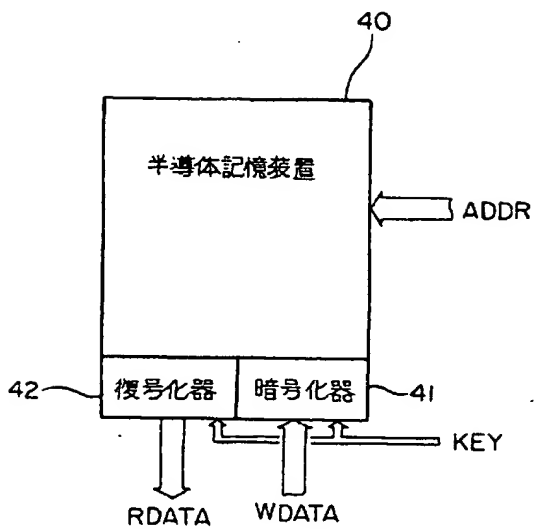


第 4 図



第 6 図

第 5 図

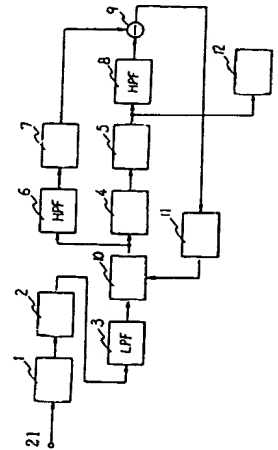


(54) IMAGE SIGNAL PROCESSING CIRCUIT

(11) 4-163767 (A) (43) 9.6.1992 (19) JP
 (21) Appl. No. 2-291598 (22) 29.10.1990
 (71) NEC CORP (72) TAKESHI KUWAJIMA
 (51) Int. Cl⁵. G11B20/06, H04N5/92

PURPOSE: To cancel the effect of phase shift delay due to a non-linear circuit and a low pass filter, and reproduce an excellent image luminance signal by extracting high pass components before and after de-emphasize processing and conducting phase shift correction on a signal before the de-emphasize processing with the differential output of the signals before and after the de-emphasize processing as a control input.

CONSTITUTION: The output of a nonlinear de-emphasize circuit 5 is inputted to a high pass filter 8 to remove DC components. Differential output between the output of a limiter circuit 7 and the output of the high pass filter 8 is obtained by a subtracter 9 to be inputted to a control circuit 11. The control circuit 11 gives a phase shift circuit 10 the operating point of phase shift quantity control with the output of the subtracter 9 as control input. At this time, the control circuit 10 outputs such a control output as to correct the phase shift quantity of the phase shift circuit 10 so that, for instance, the differential output of the subtracter 9 may be zero. Thus, the reproducibility of edge component or the like can be improved.



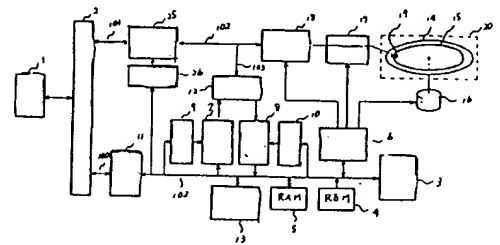
1: limiter circuit, 2: FM demodulating circuit, 4: main de-emphasize circuit, 12: reproduced signal processing circuit, 21: reproduced FM signal

(54) DISK SECURITY SYSTEM AND APPARATUS

(11) 4-163768 (A) (43) 9.6.1992 (19) JP
 (21) Appl. No. 2-288528 (22) 29.10.1990
 (71) HITACHI LTD (72) MITSUO OYAMA(1)
 (51) Int. Cl⁵. G11B20/12, G11B20/00

PURPOSE: To perform disk security by recording encryption of management information recorded in a management storage.

CONSTITUTION: When a user gets access to a storage medium 14, an encryption key and a decoding key are inputted and, when a file is anew written in, further a data translation key is inputted. When file management information is written in the storage medium 14, the file management information encrypted by using the inputted encryption key and an encryption circuit 7 is written in the storage medium 14. On the contrary, when the file management information is read out, a cryptogram is translated to a plaintext by using the decoding key and a decoding circuit 8. Therefore, since one who does not know the encryption key and the decoding key can not get access to the file management information, it is difficult to duly get access to the file in the storage medium 14 after all and the file management information in the storage medium is encrypted. Thus, security is enabled on the storage medium 14 by itself.



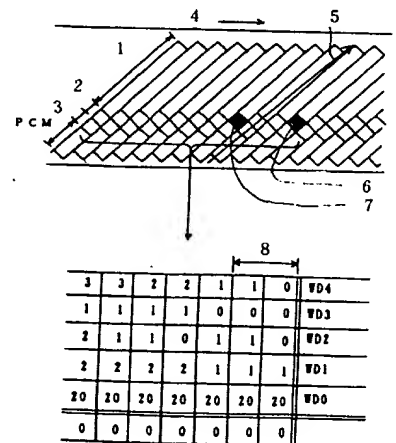
1: host computer, 2: interface, 3: microprocessor, 6: control interface, 7: encryption circuit, 8: decoding circuit, 9: encryption key register, 11: processor interface, 12: buffer interface, 13: copy storing memory for file control information, 16: motor, 17: actuator mechanism, 18: read/write circuit, 25: data conversion/restoration circuit, 26: data converting key register, 100: command, 101: data, 102: converting data

(54) SIGNAL RECORDER

(11) 4-163769 (A) (43) 9.6.1992 (19) JP
 (21) Appl. No. 2-291470 (22) 29.10.1990
 (71) CANON INC (72) HIROO EDAKUBO(2)
 (51) Int. Cl⁵. G11B20/12, G11B15/087, G11B27/28

PURPOSE: To rapidly search a plurality of the pieces of main information by recording index signals over a given section in an index recording area for every index and making the index signals provide a plurality of the pieces of index number data for distinguish the indexes one from another for every track.

CONSTITUTION: Index signals are recorded over a given section in an index recording area for every index. A plurality of the pieces of index number data are provided wherein the index signals distinguish indexes from one another for every track. Therefore, since the same index number is applied to the track of the given section, even when a tape-like recording medium is fed at high speed, a track group with the target index number can be surely searched. Moreover, a different index number can be applied for every given section and main information for a plurality of the indexes can be surely searched in a short time. Thus, even when a plurality of the pieces of target main information are present in temporal proximity, these pieces of the target main information can be accurately searched in a short time.



1: image signal, 2: data, 3: header, 1: tape running direction, 5: drum rotating direction, 6: index #1, 7: index #2, 8: one frame

Best Available Copy

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A) 平4-163768

⑬ Int. Cl.⁵

G 11 B 20/12
20/00

識別記号

Z

庁内整理番号

9074-5D
9197-5D

⑭ 公開 平成4年(1992)6月9日

審査請求 未請求 請求項の数 4 (全7頁)

⑮ 発明の名称 ディスク機密保護方式および装置

⑯ 特 願 平2-288528

⑰ 出 願 平2(1990)10月29日

⑱ 発 明 者 大 山 光 男 東京都国分寺市東恋ヶ窪1丁目280番地 株式会社日立製作所中央研究所内

⑲ 発 明 者 荒 澤 伸 幸 東京都国分寺市東恋ヶ窪1丁目280番地 株式会社日立製作所中央研究所内

⑳ 出 願 人 株式会社日立製作所 東京都千代田区神田駿河台4丁目6番地

㉑ 代 理 人 弁理士 小川 勝男 外1名

明 細 書

1. 発明の名称

ディスク機密保護方式および装置

2. 特許請求の範囲

1. ディスク記憶媒体上に、ファイルを記憶するファイル記憶部と、ファイル記憶部へのファイルの記憶を管理制御する管理情報を記憶するための管理情報記録部とを有してなるディスク記憶媒体において、ファイル記憶部に記憶するデータを、データ変換鍵により一意的に定まるデータ変換手順によりデータ変換したデータとし、管理情報記録部に記憶される管理情報を、少なくとも、ファイルを識別するためのファイル名と、ファイルの長さ、ファイルのロケーションと、該データ変換鍵とを含んで構成し、かつ管理記憶部に記録する該管理情報を暗号化して記録することを特徴とするディスク機密保護方式。

2. カートリッジ内にディスク記憶媒体と、半導体メモリを具備して成り、ディスク記憶媒体上

にファイルを記憶し、ディスク記憶媒体へのファイルの記憶を管理制御するための管理情報を該半導体メモリに記憶するディスクカートリッジにおいて、ディスク記憶媒体に記憶するデータを、データ変換鍵により一意的に定まるデータ変換手順によりデータ変換したデータとし、該半導体メモリに記憶するファイル管理情報は、少なくとも、ファイルを識別するためのファイル名、ファイルの長さ、ファイルのロケーション、該データ変換鍵を含んで構成し、かつ該半導体メモリに記録する該管理情報を暗号化して記録することを特徴とするディスク機密保護方式。

3. 請求項1記載のディスク記憶媒体が装着され、該ディスク記憶媒体にファイルをリード/ライトするディスク記憶装置において、暗号化鍵の入力手段と、復号鍵の入力手段と、データ変換鍵の入力手段と、該データ変換鍵をファイル管理情報の構成要素として登録する手段と、該データ変換鍵により一意的に定まるデータ変換手

段によりデータ変換を行う手段と、データ変換されてディスク記憶媒体に記憶されたデータを、該データ変換鍵を用いて復元する手段と、ファイル管理情報を、入力された該暗号化鍵を用いて暗号化し、管理情報記録部に書き込む手段と、管理情報記録部に暗号化して記録されている管理情報を読みだし、入力された該復号鍵を用いて暗号を解読し、平文に変換する手段とを備えたことを特徴とするディスク記憶装置。

4. 請求項2記載のディスクカートリッジが装着され、該ディスクカートリッジにファイルをリード/ライトするディスク記憶装置において、暗号化鍵の入力手段と、復号鍵の入力手段と、データ変換鍵の入力手段と、該データ変換鍵をファイル管理情報の構成要素として登録する手段と、ディスク記憶媒体に記憶するデータを該データ変換鍵により一意的に定まるデータ変換手順によりデータ変換する手段と、データ変換されてディスク記憶媒体に記憶されたデータを、該データ変換鍵を用いて復元する手段と、管理

情報を、入力された該暗号化鍵を用いて暗号化し、ディスクカートリッジに内蔵される半導体メモリに書き込む手段と、該半導体メモリから暗号化して記録された管理情報を読みだし、入力された該復号鍵を用いて暗号を解読し、平文に変換する手段とを備えたことを特徴とするディスク記憶装置。

3. 発明の詳細な説明

(産業上の利用分野)

本発明は、特に着脱可能な記憶媒体、例えばフロッピディスク、光ディスク等に好適な機密保護方式および装置に関する。

(従来の技術)

近年、重要なデータが多量にコンピュータシステムに蓄積されるようになり、重要情報、機密情報の漏洩、破壊が大きな問題になってきている。このような状況にあって、機密保護の簡便な方式としてパスワードが用いられてきた。すなわち、OS (オペレーティングシステム) の管理のもとにパスワードを登録しておき、ユーザは、システ

ムを利用する際パスワードを入力し、OSは登録されているパスワードとユーザが入力したパスワードを比較し、一致すればシステムの利用を許可するようにしていた。しかし、この方法では、記憶装置に着脱可能な記憶媒体、たとえばフロッピディスクや光ディスクでは、記憶媒体自身では機密保護機能を持たないので、他のシステムでは第三者がアクセスでき、機密保護はなされない。

これを防ぐため、特開平1-159724号公報で開示されている方式では、記憶媒体からファイル読み出す際に、ファイルに付加されているパスワードと、ユーザが入力したパスワードを照合し、一致したときのみファイルの読みだしを許可するようにしている。また、特開平1-308120号公報で開示されている方式では、記憶媒体にパスワードをマウントしておき、記憶媒体イニシャライズの際、入力されたパスワードと記憶媒体にマウントされたパスワードを照合し、一致したときのみイニシャライズを実行している。

(発明が解決しようとする課題)

特開平1-159724号公報、特開平1-308120号公報で開示されている方式では、パスワードを照合する機能を備えた記憶装置に装着して使用されるかぎり、パスワードを知らない者のファイル読みだし、あるいは、記憶媒体のイニシャライズを防ぐことができる。しかし、記憶装置に着脱可能な記憶媒体、例えばフロッピディスク、光ディスクなどでは、記憶媒体を装着する記憶装置がパスワードの照合機能を持っていないか、あるいは、故意にパスワードの照合を省略した場合は、ファイルの内容を容易に読みだし、あるいはイニシャライズすることができる。すなわち、記憶媒体自体は機密保護機能を持っておらず、十分な機密保護ができない場合がある。

本発明の目的は、記憶媒体自体に機密保護機能を付加し、第三者が容易にアクセス出来ないようにして、機密保護機能を強化することにある。

(課題を解決するための手段)

上記目的を達成するために、本発明では、

- (1) 記憶媒体上に、少なくとも、ファイル名、フ

ファイルのサイズ、ロケーション、データ変換鍵を含んで構成されるファイル管理情報を暗号化して登録し、

- (2) 記憶媒体にファイルを記憶する際、データ変換鍵により一意的に定まるデータ変換手順によってデータ変換して記録するようにした。

さらに、本発明では、上記方式を実現するための記憶装置を提供する。すなわち、着脱可能なフロッピディスク、光ディスク等を記憶媒体とするディスク記憶装置において、暗号化回路、復号回路、暗号化鍵入力手段、復号鍵入力手段、データ変換鍵入力手段、データ変換／データ復元回路を設けた。そして、記憶媒体上のファイル管理情報を暗号化して記録するようにした。

〔作用〕

ユーザは、記憶媒体にアクセスする際、暗号化鍵、復号鍵を入力し、新たにファイルを書き込む場合にはさらにデータ変換鍵を入力する。そして、本発明による記憶装置は、記憶媒体にファイル管理情報を書き込む場合、入力された暗号化鍵と暗

号化回路を用いて暗文に変換して書き込む。逆に、ファイル管理情報を読み出す場合は、復号鍵と復号回路により、暗文から平文に変換する。

これにより、暗号化鍵と復号鍵を知らない者はファイル管理情報にアクセスすることが出来ない。結局、記憶媒体上のファイルを正しくアクセスすることが困難になり、機密が保たれる。また、記憶媒体上のファイル管理情報が暗号化されることにより、記憶媒体自体で機密保護が可能になる。

さらに本発明では、記憶媒体にファイルを記憶する際、データ変換鍵を用いて、データ変換回路によりデータ変換して書き込み、逆に記憶媒体からファイルを読み出す際は、データ変換鍵を用いて、データ復元回路により復元して読み出す。これにより、たとえ特殊な手段により記憶媒体上のデータを直接読み出すことができた場合にも、データ変換鍵を知らなければ、正確に復元することは困難であり、機密が保護される。

また、データ変換鍵は、ファイル管理情報の構

成要素として、暗号化して記憶媒体上に記憶されるので、復号鍵を知らないとデータ変換鍵を正しく読み出すことはできない。

〔実施例〕

本発明の第1の実施例によるディスク記憶装置の構成を第1図に、第1図に示す装置の動作を説明するフローチャートを第7図に示し、以下に説明する。

第1図において、20はフロッピディスク、光ディスク等の着脱可能なディスク、14はディスク記憶媒体、15はディスク記憶媒体上のファイル管理情報格納領域、1はディスク記憶装置に装着されたディスク20にデータをリード／ライトするホストコンピュータ、2はディスク記憶装置にホストコンピュータ1を接続するためのインタフェース、3はディスク記憶装置を制御するためのマイクロプロセッサ、4はマイクロプロセッサ3で実行する制御プログラムが格納されるROM、5はマイクロプロセッサ3のワーク領域として機能するRAM、6はスピンドルモータ16、アク

チュエータ機構17、リードライト回路18を制御するための制御インタフェース、7はファイル管理領域15に書き込むデータを、暗号化鍵レジスタ9に保持される暗号化鍵を用いて暗号化するための暗号化回路、8はファイル管理領域15から読み出す暗号化されたデータを、復号鍵レジスタ10に保持される復号鍵を用いて解読し、平文に変換するための復号回路、12は速度調整用バッファメモリ、13は暗号化されていない（平文の）ファイル管理情報を格納するためのメモリ、25はデータ変換鍵レジスタ26に保持されるデータ変換鍵を用いて、ディスク記憶媒体14に記憶するファイルをデータ変換して記憶し、逆にディスク記憶媒体から読み出したデータを復元するためのデータ変換／データ復元回路である。

第5図にデータ変換／復元回路の一構成例を示す。第5図において、記憶媒体に記憶されるデータ101はN個の排他的論理和回路30-1、30-Nによりビット反転され変換データ102となり、逆に記憶媒体から読みだされた変換デー

タ102はN個の排他的論理和31-1, 31-Nにより再度ビット反転されてもとのデータ101に復元される。このとき、反転されるビットの数と位置はデータ変換鍵のビットパターンにより定まる。したがって、例えばデータ変換鍵の長さは64ビット以上あれば選択可能なビットパターンの数は膨大になり、データ変換鍵のビットパターンを知らないかぎりデータの復元は極めて困難になる。

次に、第7図に示すフローチャートを用いて第1図に示すディスク記憶装置の動作を説明する。最初にアクセス対象のディスク20をディスク記憶装置に装着し、ホストコンピュータ1よりディスク記憶装置を起動する。ユーザは、暗号化鍵、復号鍵を入力し、新たにファイルを書き込む場合は、さらにデータ変換鍵を入力する700。入力された暗号化鍵、復号鍵は、インタフェース2、コマンド線101、プロセッサインタフェース11を介して、マイクロプロセッサ3により暗号化鍵レジスタ9、復号鍵レジスタ10にセットさ

れる。マイクロプロセッサ3は、ディスク記憶媒体14上のファイル管理領域15から暗号化されたファイル管理情報を読みだし、復号鍵を用いて復号回路8により暗号を解読して平文に変換し、ファイル管理情報の写し格納メモリ13に格納する701。ホストコンピュータからリード/ライト要求を受けると、マイクロプロセッサ3は、ファイル管理情報の写し格納メモリ13からファイル管理情報を読み取り、アクセスすべきファイルの属性、サイズ、ロケーション、データ変換鍵等の情報を得、データ変換鍵をデータ変換鍵レジスタ26にセットする702。

次に、マイクロプロセッサ3は、読み取ったファイル管理情報をもとに、ホストコンピュータ1との間でインタフェース2を介して、リード/ライトデータのやりとりを行い、ライトの場合は、データ変換/データ復元回路25、リード/ライト回路18を介して変換データをディスク記憶媒体14に書き込む。一方、リードの場合はリード/ライト回路18を介してディスク記憶媒体14

から読み出した変換データ102をデータ変換/復元回路25により復元して101、ホストコンピュータ1に読み出す703。次に、ディスクへのリード/ライトを行った結果、ファイル管理情報の更新が必要かどうかを調べる604。そして、更新が必要であれば、ファイル管理情報の写し格納メモリ13の内容を更新するとともに、暗号化鍵を用いて暗号化回路7により更新内容を暗号化してディスク記憶媒体14上のファイル管理領域15の内容を更新する。そしてこのとき、ファイルの新たな書き込みがあった場合は、そのとき使用したデータ変換鍵をファイル管理情報として登録し、暗号化してディスク記憶媒体14に記憶する705。

以上に説明したディスク記憶装置の制御は、制御プログラムとして記述され、ROM4に格納されており、マイクロプロセッサ3で実行することにより実現される。

このように、ファイル管理情報を暗号化しておくことにより、暗号化鍵、復号鍵を持つ者以外は

ファイル管理情報を読むことができないので、所望のファイルのサイズ、ロケーション、属性等がわからず、ディスク記憶媒体へのリード/ライトを正しく行うことが困難になり、機密が保護される。

また、データ変換鍵がファイル管理情報の構成要素としてディスク記憶媒体14に記憶されるので、新たにファイルを書き込む場合以外はデータ変換鍵を入力する必要がなく、かつデータ変換鍵は暗号化して記憶されるので、ディスク記憶媒体からファイル管理情報を読みだせた場合にも、データ変換鍵を解読することは困難であり、機密が保護される。

以上、本発明の第1の実施例では、ファイル管理情報がディスク記憶媒体14上に記録される場合について説明した。しかし、ファイル管理情報がディスク記憶媒体14上に記録されると、ファイル管理情報を更新する毎にディスク記憶媒体14上のファイル管理領域15にアクセスすることが必要になり、ディスクのリード/ライトのスト

ループットが低下する。これを避けるため、第4図に示すように、ディスクカートリッジ21に高速半導体メモリ22を埋め込み、この半導体メモリ22にファイル管理情報を格納する方式がある。この場合、この半導体メモリ22に格納するファイル管理情報を暗号化し、ディスク記憶媒体14に、データ変換を施した変換データを記憶することにより、ディスクカートリッジ21自体で機密保護を行うことができる。

第6図は、本発明の第2の実施例によるディスク記憶装置の構成を示す図、第8図はその動作を説明するフローチャートである。第6図において、21はディスクカートリッジであり、第4図に示すように、データを記録するディスク記憶媒体14とは別に、カートリッジに埋め込まれた半導体メモリ22を有しており、暗号化したファイル管理情報が格納される。23は外部から半導体メモリ22にアクセスするためのコネクタである。

第6図に示すディスク記憶装置において、暗号化されたファイル管理情報の入出力が、コネクタ

23を介してカートリッジに埋め込まれた半導体メモリ22に対して行われること、およびファイル管理情報の写し格納領域が必要に応じてRAM5上に設けられること以外は第1図に示すディスク記憶装置に同じである。半導体メモリのアクセス時間は、ディスクのアクセス時間に比べて一般に十分短い。したがって、復号回路8による暗号の解読が十分速く実行できれば、半導体メモリ22に格納されている管理情報の写しをRAM5上に持つ必要はなく、直接半導体メモリ22をアクセスすればよい。

なお、以上の説明では、暗号化鍵と復号鍵が異なる、公開鍵暗号による暗号化を行う場合について説明したが、秘密鍵暗号による暗号化を行う場合は、暗号化鍵と復号鍵は共通であるので、暗号化鍵レジスタ9と復号鍵レジスタ10は共通にできる。

〔発明の効果〕

以上に説明したように、本発明によればディスクカートリッジ、あるいはディスク記憶媒体自体

が機密保護機能を持つので、パスワードを付加する方式に比べ、特に着脱可能なディスク記憶媒体において、機密保護機能が強化されるという効果がある。

4. 図面の簡単な説明

第1図は第1の実施例によるディスク記憶装置の構成を示す図、第2図は本発明の方式を説明する図、第3図はファイル管理情報の構成例を示す図、第4図は半導体メモリを有するディスクカートリッジを示す図、第5図はデータ変換/復元回路の一構成例を示す図、第6図は第2の実施例によるディスク記憶装置の構成を示す図、第7図は第1図に示す装置の動作を説明するフローチャート図、第8図は第6図に示す装置の動作を説明するフローチャート図である。

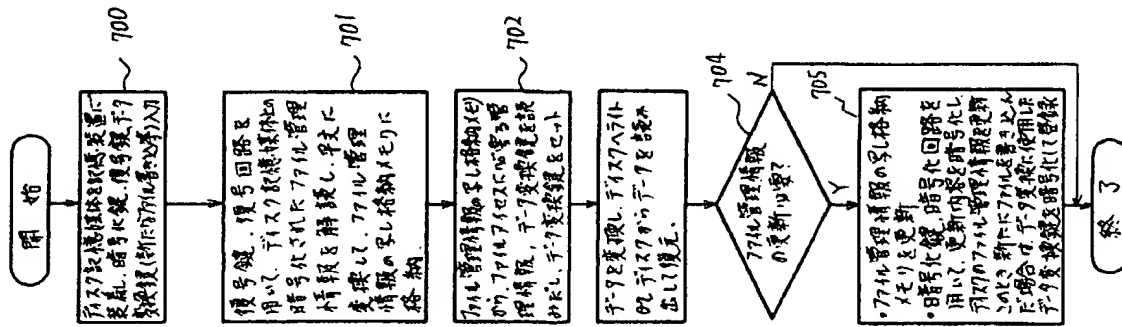
1…ホストコンピュータ、3…マイクロプロセッサ、4…ROM、5…RAM、7…暗号化回路、8…復号回路、9…暗号化鍵レジスタ、10…復号鍵レジスタ、12…バッファメモリ、13…ファイル管理情報の写し格納メモリ、20…ディス

ク、21…半導体メモリを有するディスクカートリッジ、22…半導体メモリ、23…コネクタ、25…データ変換鍵レジスタ、26…データ変換/復元回路。

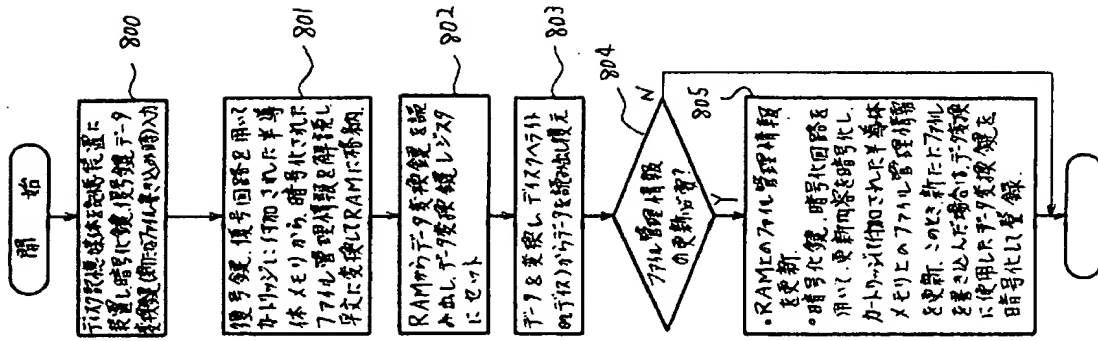
代理人 弁理士 小川勝男



第 7 図



第 8 図





PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09044407 A**(43) Date of publication of application: **14 . 02 . 97**

(51) Int. Cl.

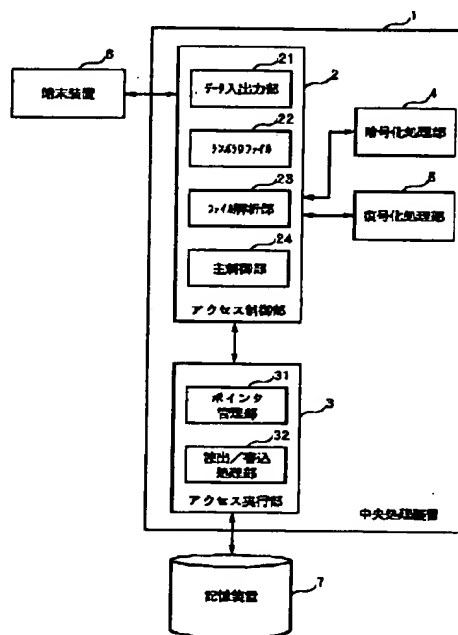
G06F 12/14
G06F 12/00(21) Application number: **07197778**(71) Applicant: **NEC ENG LTD**(22) Date of filing: **02 . 08 . 95**(72) Inventor: **ISHIBASHI MAKOTO****(54) METHOD FOR PROTECTING DATA FILE AND SECURITY SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To surely prevent the leakage of data file contents by making unauthorized access meaningless in a system provided with a highly confidential data file.

SOLUTION: This system is provided with an access execution part 3 for reading the data file requested from a user, an access control part 2 for controlling a password and managing where in a storage device 7 the record of the data file is positioned, a ciphering processing part 4 for ciphering the address of a record pointer and a deciphering processing for deciphering the address of the record pointer. The password is set for a data file unit, the password for setting the address of the next record pointer for connecting the respective records of the data file is ciphered as a key and the address can not be deciphered as long as the password is not inputted.

COPYRIGHT: (C)1997,JPO



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-44407

(43)公開日 平成9年(1997)2月14日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 B
				3 2 0 C
12/00	5 3 7	7623-5B	12/00	5 3 7 H

審査請求 未請求 請求項の数 3 O L (全 6 頁)

(21)出願番号 特願平7-197778

(22)出願日 平成7年(1995)8月2日

(71)出願人 000232047

日本電気エンジニアリング株式会社
東京都港区芝浦三丁目18番21号

(72)発明者 石橋 誠

東京都港区芝浦三丁目18番21号 日本電気
エンジニアリング株式会社内

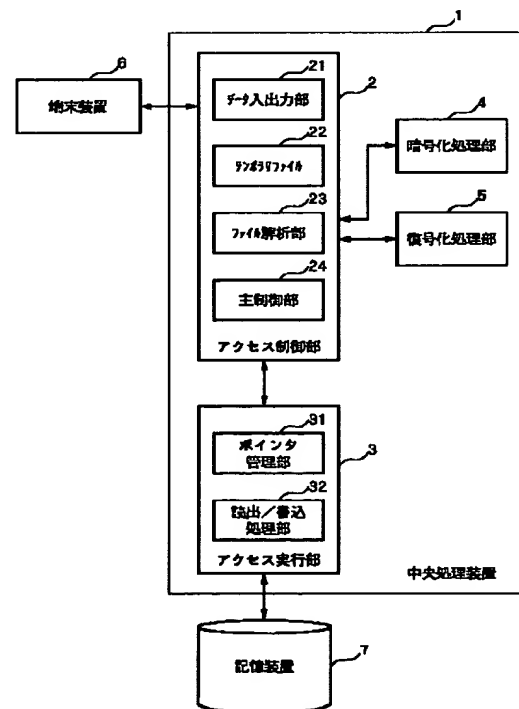
(74)代理人 弁理士 鈴木 正剛

(54)【発明の名称】 データファイルの保護方法及びセキュリティ方式

(57)【要約】

【課題】 機密性の高いデータファイルをもつシステムにおいて、不正なアクセスを無意味にしてデータファイル内容の漏洩を確実に防止する。

【解決手段】 利用者から要求のあるデータファイルを読み出すアクセス実行部3と、パスワードの制御やデータファイルのレコードが記憶装置7のどこに位置するかを管理するアクセス制御部2と、レコードポイントのアドレスを暗号化する暗号化処理部4と、レコードポイントのアドレスを復号化する復号化処理部5を備え、データファイル単位にパスワードを設定し、データファイルの各レコードを結び付ける次レコードポイントのアドレスを上記設定したパスワードを鍵として暗号化するとともに、このパスワードを入力しない限り上記アドレスを復号化できないようにした。



【特許請求の範囲】

【請求項 1】 記憶装置に格納するデータファイル単位にパスワードを設定しておき、該データファイルに含まれるレコードが複数のときに一のレコードに後続する次レコードの格納領域を指標する次レコードポインタのアドレスを前記設定したパスワードで暗号化して前記一のレコードに付加し、該データファイルの読出時には、前記パスワードを復号鍵として前記一のレコードに付加されている次レコードポインタのアドレスを復号化することを特徴とするデータファイルの保護方法。

【請求項 2】 記憶装置への格納対象となるデータファイル及び該データファイル固有のパスワードを受け付ける手段と、

受け付けたデータファイルに含まれるレコードの格納領域を指標するレコードポインタのアドレスを決定する手段と、

前記レコードが複数のときに一のレコードに後続する次レコードのレコードポインタのアドレスを前記パスワードで暗号化する手段と、

暗号化したアドレスを前記一のレコードに付加する手段と、

前記レコードを含むデータファイルを前記記憶装置に格納する手段とを備えることを特徴とするデータファイルのセキュリティ方式。

【請求項 3】 請求項 2 記載のセキュリティ方式により前記記憶装置に格納されたデータファイルの読出要求及び該データファイル固有のパスワードを受け付ける手段と、

該データファイルに含まれる各レコードのレコードポインタのアドレスを前記受け付けたパスワードを復号鍵として復号化する手段と、

復号化されたアドレスに基づいて前記データファイル内の各レコードを読み出す手段とを備えることを特徴とするデータファイルのセキュリティ方式。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、情報処理装置の記憶装置に格納された、機密性の高いデータファイルへの不正なアクセス（読出／書込、以下同じ）を防止する技術に関する。

【0002】

【従来の技術】 複数の利用者が任意にアクセス可能なデータファイルを保持する情報処理システムのセキュリティ方式として、利用者の認証チェックをシステム利用時に行って不正利用者によるログインを制限する方式と、データファイルへ実際にアクセスする際に利用者資格のチェックを行って無資格者によるアクセスを制限する方式とが知られている。

【0003】 前者の方式は、利用者がシステムにログインする際にパスワードを入力し、この入力パスワードが

予めパスワード情報ファイルに登録されたパスワードと一致するか否かをチェックし、一致する場合のみシステム利用を許可する方式である。一方、後者の方式には、データファイル毎にパスワードを設定しておき、利用者が該データファイルにアクセスする際に入力したパスワードと上記設定したパスワードとの一致性を比較することで利用者の資格をチェックし、正当の場合にのみアクセス権を与える方式と、利用者毎に利用者資格の ID を事前に割り振っておき、各データファイルに設定された利用者資格 ID と利用者が入力した ID との一致性をアクセス時にチェックして正当の場合にのみアクセス権を与える方式とがある。

【0004】

【発明が解決しようとする課題】 上述のいずれの方式も、事前に設定した利用者単位、あるいはデータファイル単位のパスワードや利用者資格 ID をシステム内のパスワード情報ファイルや利用者資格 ID 情報ファイルで管理している。この場合に、パスワード等の機密性を十分に高くしないと不正利用者にパスワード等の解読がなされ、データファイルのアクセス権が悪意の利用者へ与えられてしまう。そのため、このような機密性の高い情報の管理には十分な配慮が必要とされていた。

【0005】 そこで、本発明は、パスワード等の機密性の高い情報に対する不正アクセスを確実に防止し、システムのセキュリティ運用の向上を図る技術を提供することにある。

【0006】

【課題を解決するための手段】 上記課題を解決するため、本発明は、データファイルの保護方法を提供する。この方法は、記憶装置に格納するデータファイル単位にパスワードを設定しておき、該データファイルに含まれるレコードが複数のときに一のレコードに後続する次レコードの格納領域を指標する次レコードポインタのアドレスを前記設定したパスワードで暗号化して前記一のレコードに付加し、該データファイルの読出時には、前記パスワードを復号鍵として前記一のレコードに付加されているアドレスを復号化することを特徴とする。

【0007】 本発明は、また、上記方法を実現する、データファイルのセキュリティ方式をも提供する。この方式は、データファイルを格納する方式と読み出す方式とに分かれる。データファイルを格納する方式は、記憶装置への格納対象となるデータファイル及び該データファイル固有のパスワードを受け付ける手段と、受け付けたデータファイルに含まれるレコードの格納領域を指標するレコードポインタのアドレスを決定する手段と、前記レコードが複数のときに一のレコードに後続する次レコードのレコードポインタのアドレスを前記パスワードで暗号化する手段と、暗号化した次レコードポインタアドレスを前記一のレコードに付加する手段と、前記レコードを含むデータファイルを前記記憶装置に格納する手段

とを備える。

【0008】一方、データファイルを読み出す方式は、上記格納方式により前記記憶装置に格納されたデータファイルの読出要求及び該データファイル固有のパスワードを受け付ける手段と、該当データファイルに含まれる各レコードのレコードポインタのアドレスを前記受け付けたパスワードを復号鍵として復号化する手段と、復号化されたアドレスに基づいて前記データファイル内の各レコードを読み出す手段とを備える。

【0009】このような構成のセキュリティ方式では、読み出しの際に、正しいパスワードを与えない限り、データファイル内の各レコードに関連付けるレコードポインタのアドレスが正しく復元されないので、パスワードを知らない者によるデータファイルの不正アクセスを防止することができる。

【0010】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を詳細に説明する。図1は、本発明の一実施形態である情報処理システムの構成図である。この情報処理システムは、記憶装置7が接続された中央処理装置1と、この中央処理装置1にアクセス可能に接続された少なくとも一つの端末装置6とから構成される。中央処理装置1は、端末装置6からのアクセスを制御するアクセス制御部2と、記憶装置6へのアクセスを実行するアクセス実行部3と、暗号化処理部4と、復号化処理部5とを備えている。

【0011】アクセス制御部2は、端末装置との間のデータ入出力やパスワードの入力を行うデータ入出力部21と、パスワードを一時的に保持するテンポラリファイル22と、端末装置6から受け付けたデータファイルの内容を解析するファイル解析部23と、上記各部その他の制御を司る主制御部24とから構成される。また、アクセス制御部3は、記憶装置7内のレコード格納領域を指標するレコードポインタのアドレスを管理するポインタ管理部31と、記憶装置7へのデータファイルの読出又は書込を行う読出／書込処理部32とから構成される。

【0012】記憶装置7には、図2に示すように、ファイルラベル8と、レコード部9とが格納されている。ファイルラベル8は、複数のデータファイルのファイル名やファイル属性、実際に書き込まれているレコードのアドレスを示すレコードポインタエリア等から構成される。1データファイルについて1つのファイルラベル8が存在する。

【0013】レコード部9は、各データファイルのデータ内容が書き込まれるレコード群から成る。各レコードについて関連する後続のレコードが存在する場合、当該レコードの次レコードポインタエリアに、次レコードポインタのアドレスが書き込まれる。図2の例では、ファイルA～ファイルCのファイルラベルに各々レコードポ

インタNPのアドレスが書き込まれており、さらに、ファイルAについては、2つの連続するレコードA-1、A-2が存在している。このときファイルAの最初のレコードA-1の次コードポインタエリアに、次レコードポインタNPのアドレスが書き込まれる。ファイルCについても同様となる。なお、ファイルBのレコードは一つだけなので、レコードB-1における次レコードポインタエリアは空白となる。

【0014】次に、本実施形態による情報処理システムの動作を具体的に説明する。端末装置6から記憶装置7へデータファイルを新規に作成する旨の要求がアクセス制御部2のデータ入出力部21に入力されると、主制御部24はこれを検出して、暗号鍵となるパスワードの入力を当該端末装置6（利用者）に促す。端末装置6からパスワードが入力された場合は、これを一時テンポラリファイル22に保持するとともに、データファイル内容を受け付けてファイル解析部24に渡す。

【0015】ファイル解析部23は、この受け付けたデータファイル内のレコード数やその関連を調べ、さらにアクセス実行部3のポインタ管理部31よりレコードポインタのアドレスを取得する。そして、一のレコードについて次レコードが存在する場合は、ポインタ管理部31より取得したそのままのアドレスをデータとして書き込まず、これを暗号化処理部4に渡す。暗号化処理部4は、テンポラリファイル22に保持されている入力パスワードを暗号鍵としてアドレスの暗号化を行う。暗号化には任意の方式を用いることができる。本実施形態では公知のDES方式を使用する。ファイル解析部23は、暗号化されたアドレスを暗号化処理部4より受け取って当該一のレコードの次レコードポインタエリアへ書き込む。書込が終了すると、主制御部24は、このレコードを含むデータファイルをアクセス実行部3に送り、テンポラリファイル22が保持していたパスワードを消去する。アクセス実行部3では、アクセス制御部2より送られたデータファイルを読出／書込処理部32が記憶装置7の該当アドレスに書き込む。

【0016】この操作により書き込まれたデータファイルは、各レコードの関連を示す、次レコードポインタエリアに示されるアドレスが暗号化されることにより、各レコード間の関連性が判らなくなっており、これを単に読み出そうとしても情報としての意味をなさなくなる。つまりデータファイルのセキュリティ性が確保される。

【0017】一方、端末装置6からデータファイルの読出、更新、あるいは削除を行う旨の要求がアクセス制御部2に入力された場合は、主制御部24が当該端末装置（利用者）6へ、各データファイルを作成した際に使用したパスワードの入力を促す。このとき入力されたパスワードが正しければ、参照しようとするデータファイルのファイルラベル8にある暗号化されたアドレスをアクセス実行部3経由で記憶装置7から読み出し、これを復

号化処理部 5 に渡す。復号化処理部 5 は、該パスワードを復号鍵としてアドレスを復号化する。主制御部 2 4 は、この復号化されたアドレスをアクセス実行部 3 へ送る。アクセス実行部 3 は、このアドレスをもとに次レコードの内容を読み出す。更に次のレコードが存在する場合は、そのレコードについて書き込まれている暗号化されたアドレスを同様の手順で復号化し、これをアクセス実行部 3 へ渡すことにより当該レコードの内容を読み出す。

【0018】データファイルの内容を読み出した後に更新又は削除する場合は、レコードの数が変わるが、これについては、次レコードポインタエリアのアドレスを前述のデータファイル作成と同様の手順で暗号化することによって対応することができる。

【0019】データファイルの読み出しの際に、誤ったパスワードがアクセス制御部 2 へ入力された場合、復号化されたアドレスの内容は不実となり、アクセス実行部 3 は、誤ったアドレスの内容で記憶装置 7 を読み出そうとする。しかし、そのアドレスが実際のレコード部 9 の範囲以外を示したり、レコードフォーマットに合っていないデータを読み出した場合は、利用者による端末装置 6 の不正操作としてデータファイルのアクセス処理を停止する。これにより、正しいパスワードをアクセス制御部 2 へ与えない限り、各レコードを関連付けるアドレスが正しく復元されず、正しい内容をアクセスすることが不可能になる。

【0020】なお、データファイル作成時にパスワードを設定しない場合は、「パスワードなし」をベースに次レコードポインタのアドレスを暗号化し、データファイルを読み出す場合には、「パスワードなし」で復号化することになる。このようにすれば、パスワードを設定しないデータファイルを作成する際に、上記一連の処理の*

*変更を行わなくてもデータファイルアクセスが可能になる。

【0021】

【発明の効果】以上の説明から明らかなように、本発明では、データファイル単位にパスワードを設定し、データファイルの各レコードを結びつける次レコードポインタのアドレスを上記パスワードで暗号化して各レコードの關係に機密性を持たせ、不正なデータファイルのアクセスについてはこれを無意味にするようにしたので、パスワード等の漏洩が確実に防止される効果がある。また、従来のようにパスワード情報保存用ファイル等が不要になるので、管理効率上も有利となる。

【図面の簡単な説明】

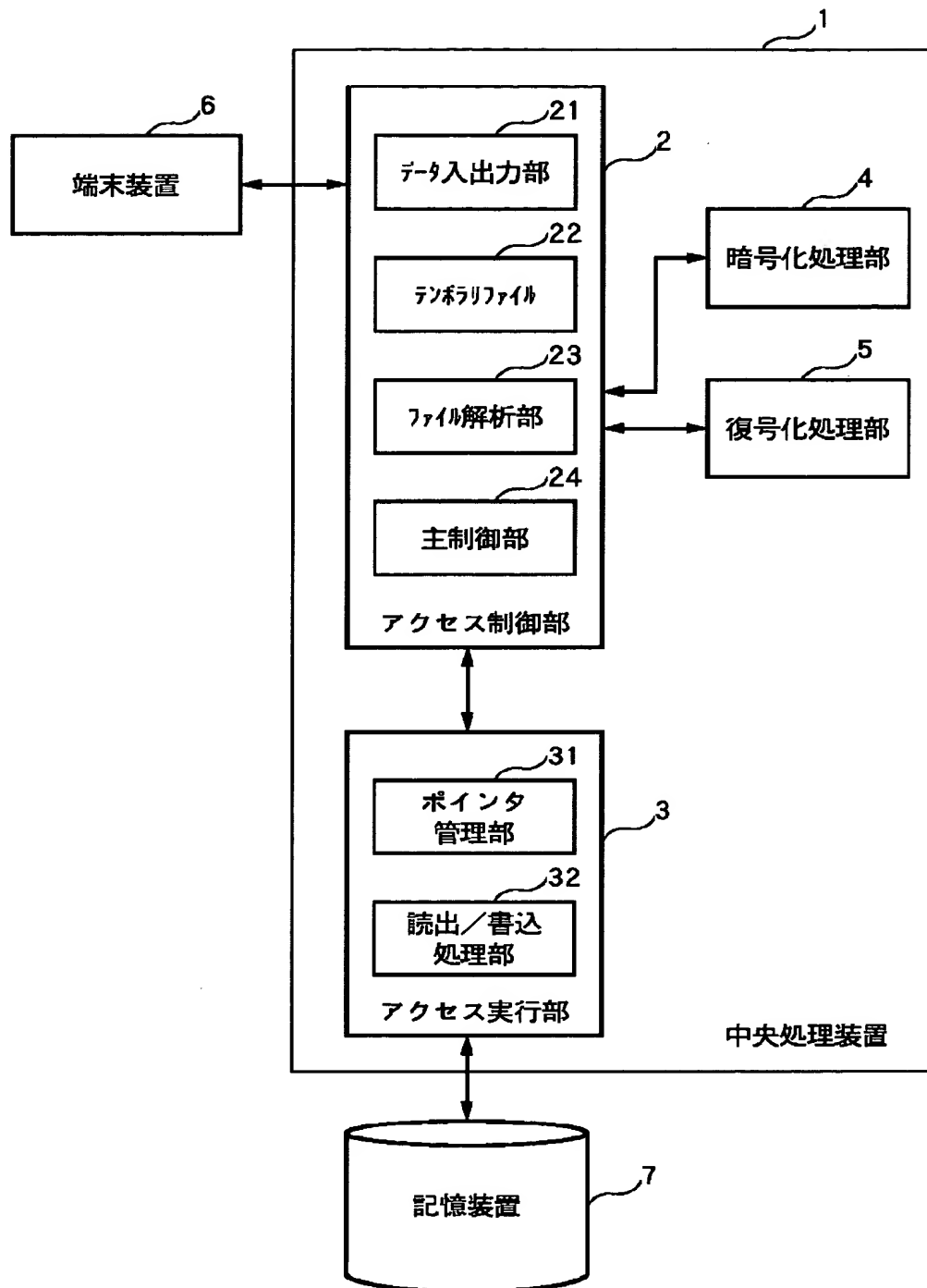
【図 1】本発明の一実施形態のセキュリティシステムの構成図。

【図 2】本実施形態による記憶装置のファイル構成図。

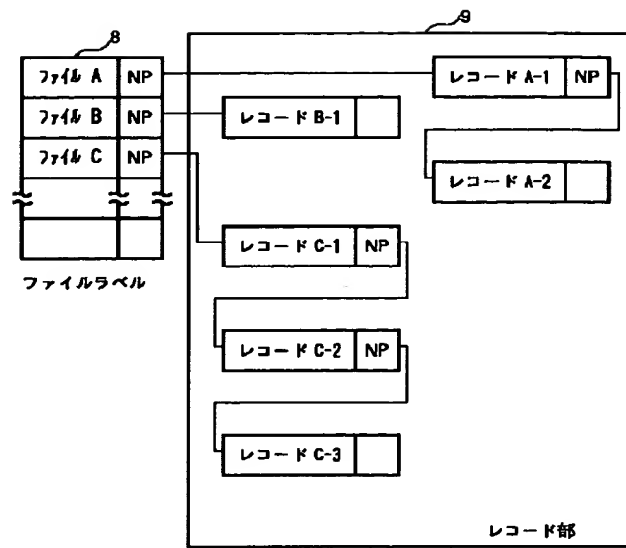
【符号の説明】

- | | |
|-----|-----------|
| 1 | 中央処理装置 |
| 2 | アクセス制御部 |
| 2 1 | データ入出力部 |
| 2 2 | テンポラリファイル |
| 2 3 | ファイル解析部 |
| 2 4 | 主制御部 |
| 3 | アクセス実行部 |
| 3 1 | ポインタ管理部 |
| 3 2 | 読出／書込処理部 |
| 4 | 暗号化処理部 |
| 5 | 復号化処理部 |
| 6 | 端末装置 |
| 7 | 記憶装置 |
| 8 | ファイルラベル |
| 9 | レコード部 |

【図 1】



【図2】



NP : 次レコードポインタ

(54) ADDRESS CONVERTER

(11) 4-149651 (A) (43) 22.5.1992 (19) JP

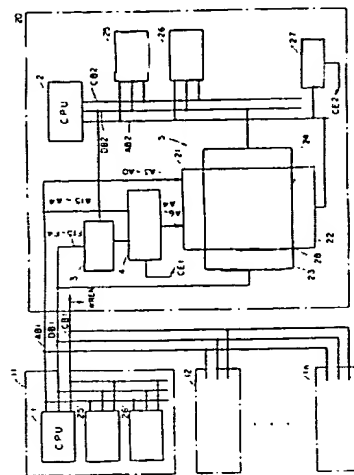
(21) Appl. No. 2-271407 (22) 8.10.1990

(71) MITSUBISHI ELECTRIC CORP (72) TATSUYA IMAKURA(1)

(51) Int. Cl⁵. G06F12/10

PURPOSE: To convert a virtual address into a real address by activating the access given to a memory cell array in response to a virtual address signal and a higher rank bit of the offset data and producing the real address signal in response to the virtual address signal and a lower rank bit of the offset data respectively.

CONSTITUTION: A microcomputer 20 including a dual port random access memory DPRAM 5 is connected to a microcomputer 11 via an address bus AB1, a data bus DB1, and a control bus CB1 respectively. A detection circuit 27 produces an activating signal CE2 when an internal address signal set in a prescribed range is applied to an address bus AB2. The access given to the DPRAM 5 from a CPU 2 is activated in response to the signal CE2. Then the microcomputer 20 converts the virtual address signal produced from a microcomputer 11 into a real address signal used for the DPRAM 5. In such a way, a virtual address signal can be converted into a real address signal with no dependence needed on the arithmetic processing jobs of the CPU 2.



11,12: microcomputer, 3: offset register, 4: address computing part, 21,22: address decoder, 23,24: sense amplifier, 25,26: function block part, 26,26': memory part, 28: DPRAM memory array

(54) MICROCOMPUTER

(11) 4-149652 (A) (43) 22.5.1992 (19) JP

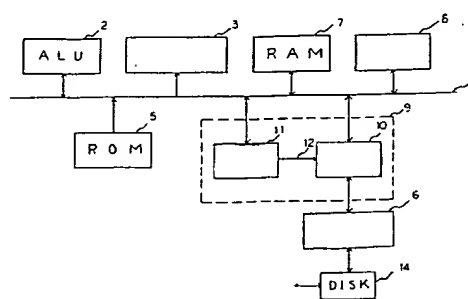
(21) Appl. No. 2-271255 (22) 9.10.1990

(71) MITSUBISHI ELECTRIC CORP (72) TAKASHI KAWARABAYASHI

(51) Int. Cl⁵. G06F12/14

PURPOSE: To read out the contents of a converting part to be ciphered to the outside by providing a bus switch circuit which ciphers the data and the programs based on the command of a data arithmetic part and the data stored in a storage part between the data arithmetic part/storage parts and an input/output part.

CONSTITUTION: A data arithmetic part ALU 2 is provided together with a ROM 5 and a RAM 7 which store the data and the programs, and an input/output part 6. Then a bus switch circuit 9 which ciphers the data and the programs is provided between the ALU 2/ROM 5 and RAM 7 and the part 6. The circuit 9 switches the arrangement of the bit trains based on the command of the ALU 2 and the data and the programs of the ROM 5 and the RAM 7 and ciphers the data and the programs. These ciphered data and programs are outputted to the outside through the part 6 and at the same time the ciphered data and programs inputted from the outside are decoded and sent to the ALU 2, the ROM 5 and the RAM 7 respectively. Thus it is not required to especially input the ciphered programs and data. Furthermore the contents of the circuit 9 can be read out and sent to the outside.



3: instruction decoding execution part, 8: peripheral function part, 11: data table

(54) READ/COMPARISON SYSTEM FOR DUPLEX MEMORY

(11) 4-149653 (A) (43) 22.5.1992 (19) JP

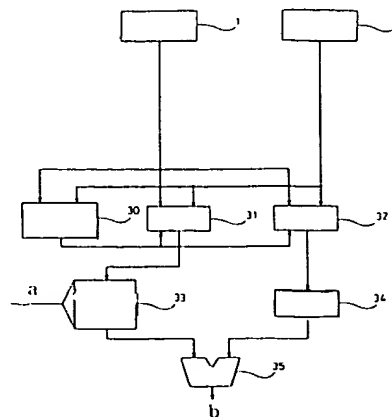
(21) Appl. No. 2-271455 (22) 9.10.1990

(71) FUJITSU LTD (72) HIROYUKI TSUJITA(1)

(51) Int. Cl⁵. G06F12/16

PURPOSE: To reduce the capacity of a buffer by controlling a selector with the output of a preceding data deciding part to store the preceding data in a data buffer and to store the subsequent data in a comparison data register respectively and comparing both data with each other by a comparator.

CONSTITUTION: The 1st and 2nd selectors 31 and 32 with the output of a preceding data deciding part 30. Then the preceding data are stored in a data buffer 33 and the subsequent data are stored in a comparison data register 34 respectively. Then the data comparison timing is secured for a comparator 35. In such a constitution, the data buffers that cause the increase of hardware can be decreased down to just a single unit. Then the capacity of the buffer storing the data read out of a duplex memory can also be reduced.



1,2: duplex memory, a: address, b: discordant output

Best Available Copy

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A) 平4-149652

⑬ Int.Cl.⁵

識別記号

庁内整理番号

⑭ 公開 平成4年(1992)5月22日

G 06 F 12/14

3 2 0 B

7629-5B

審査請求 未請求 請求項の数 1 (全6頁)

⑮ 発明の名称 マイクロコンピュータ

⑯ 特 願 平2-271255

⑰ 出 願 平2(1990)10月9日

⑱ 発 明 者 川 原 林 隆 兵庫県伊丹市瑞原4丁目1番地 三菱電機株式会社北伊丹製作所内

⑲ 出 願 人 三菱電機株式会社 東京都千代田区丸の内2丁目2番3号

⑳ 代 理 人 弁理士 宮 園 純一

明 細 書

1. 発明の名称

マイクロコンピュータ

2. 特許請求の範囲

データやプログラムの演算を行うデータ演算部と、データやプログラムを記憶する記憶部と、外部と前記データやプログラムを転送する入出力部とを備えたマイクロコンピュータにおいて、

前記データやプログラムを前記データ演算部の指令や前記記憶部内のデータに基づいて暗号化するバス切換回路を前記データ演算部及び記憶部と前記入出力部との間に介装したことを特徴とするマイクロコンピュータ。

3. 発明の詳細な説明

(産業上の利用分野)

この発明は、通信システム等の機密保護が必要なデータ処理システムで使用されるマイクロコンピュータに関するものである。

(従来技術)

第5図は従来のマイクロコンピュータのブロッ

ク図であり、同図において、1はマイクロコンピュータ内部のバス、2はALU(データ演算部)、3は命令解読実行部、4はバス1を通して命令解読実行部3に転送された暗号化命令を復号するための命令定義部、5はプログラム格納用ROM、6はマイクロコンピュータと外部とのデータの入出力を行う入出力部、7はデータ格納用RAM、8はタイマ等の周辺機能部である。ROM5やRAM7にはあらかじめ決められた順にオペコードのビット列を配置変えた暗号化したプログラムやデータが記憶されている。又命令定義部4には、暗号を復号するための命令のビット列の配置変えの手順があらかじめデータテーブルとして記憶されている。

次に動作について説明する。ROM5又はRAM7に記憶されている暗号プログラム又は入出力部6によりマイクロコンピュータの外部より供給される暗号プログラムは、バス1を通して一命令ずつ命令解読実行部3へ送られる。命令定義部4に格納されたデータテーブルに従って復号化され

る。その後、ALU 2で本来のプログラムとして実行される。

〔発明が解決しようとする課題〕

従来のマイクロコンピュータは以上のように構成されているので、復号化用のデータテーブルの内容は秘密に保つ必要があるため、命令定義部4を読み出し不可能にしなければならない。従って命令定義部4が正常に動作するのかどうかを検査するには、実際にプログラムを入力しマイクロコンピュータを動作させて間接的に確認するしかなく、適確な機能テストができなかった。また、ALU 2やRAM 7、入出力部6を通して外部と入出力されるデータは入力するプログラムの段階で暗号化することが必要で、時間と労力を必要としていた。更に入力プログラム自体の暗号化は命令定義部4のハードウェアの構成により固定されるので、安全性を高めた複雑な暗号化を行うためには、プログラムが長く、困難なものになるなどの問題点があった。

この発明は上記のような問題点を解消するため

ト列の並び切換等を行い、データやプログラムを暗号化する。暗号化したデータやプログラムが入出力部6を通して外部へ出力され、又外部から入力される前記暗号化されたデータやプログラムを復号化してデータ演算部2や記憶部5、7に転送する。

〔実施例〕

以下、この発明の一実施例を図について説明する。第1図において、1はマイクロコンピュータ内部のバス、2はALU（データ演算部）、3は命令解釈実行部、5はプログラム格納用ROM、6はマイクロコンピュータと外部とのデータの入出力を行う入出力部、7はデータ格納用RAM、8はタイマ等の周辺機能部、9はバス1と入出力部6の間に設けられたバス切換回路である。バス切換回路9は内部バス1がn本の信号線で構成されているとすると、内部バス側n本と入出力部側n本の信号線とを組合せを変更可能に接続するスイッチマトリクス10と、スイッチマトリクス10を構成する各スイッチのON/OFFを決定

になされたもので、暗号化したプログラムを入力する必要がなく、又入出力部を通してマイクロコンピュータを外部から観測する限り、プログラムやデータの全てが暗号化されており、暗号化する変換部の内容を外部へ読み出し可能としたマイクロコンピュータを得ることを目的とする。

〔課題を解決するための手段〕

この発明においては、第1図に示すように、データやプログラムの演算を行うデータ演算部2と、データやプログラムを記憶する記憶部5、7と、外部と前記データやプログラムを転送する入出力部6とを備えたマイクロコンピュータにおいて、

データやプログラムをデータ演算部2の指令や記憶部5、7内のデータに基づいて暗号化するバス切換回路9をデータ演算部2及び記憶部5、7と入出力部6との間に介装して構成した。

〔作用〕

この発明におけるマイクロコンピュータのバス切換回路9は、データ演算部2の指令や、記憶部5、7からのデータやプログラムに従って、ビッ

するデータテーブル11と、データテーブル11内のデータをスイッチマトリクス10内の各スイッチに対応するON/OFF信号として転送する信号線12とからなる。入出力部6には、例えば周辺機器としてのディスク装置14が接続され、このディスク装置14は外部の端末機等からもアクセス可能なものである。

スイッチマトリクス10及びデータテーブル11について、第2図～第4図に従って詳しく説明する。

第2図において、入力信号、出力信号が例えば8ビットであるとする、入力端子I₁～I₈がスイッチマトリクス10により切換えられて、データテーブル11が指定する出力端子O₁～O₈に接続される。これにより、マイクロプロセッサ内のデータ形式と入出力部6外のデータ形式は異なるものになる。

スイッチマトリクス10は第3図に示すスリステートバッファ群により構成され、1ビット目の入力端子I₁は8個のスリステートバッファ

G₁ ~ G₈ の全入力端に接続されている。各スリーステートバッファの出力端は出力端子 O₁ ~ O₈ に夫々接続され、各ゲートにはデータテーブル 11 から制御信号が与えられている。同様に 2 ビット目の入力端子 I₂ は次の 8 個のスリーステートバッファに接続され、データテーブル 11 からの次の 8 本の信号で制御され、出力側は 1 ビット目と同一の出力端子 O₁ ~ O₈ に夫々接続されている。

以下同様に 3 ビットから 8 ビットまでそれぞれのスリーステートバッファを夫々有し、データテーブル 11 の信号により夫々制御されるが、出力側は同一の出力端子 O₁ ~ O₈ に夫々接続される。かくして 1 ビット目の入力端子 I₁ は 8 個の出力端子 O₁ ~ O₈ のうち一本の出力端子に接続するように 8 個のスリーステートバッファ G₁ ~ G₈ のうち一個が ON とされる。第 4 図の行列式において、1 ビット目の入力端子 I₁ をいずれかの出力端子 O₁ ~ O₈ に接続するための信号を 1 列目のデータとし、2 ビット目が 2 列目のデータ、…

… 8 ビット目が 8 列目のデータとする。各列では 1 個の要素のみが “1” となり、この要素 “1” は必ず互いに異なる行に出現するようにデータテーブル 11 を設定する。要素 “1” がゲート信号として与えられるスリーステートバッファのみが ON とされる。

このような行列データがデータテーブル 11 には予め ROM 5 からの命令等により準備される。

該行列データを予め知っている当事者にとっては、入出力部 6 から読み出した暗号化プログラムやデータも外部で復号化可能である。

次に動作について説明する。マイクロコンピュータのリセット時にスイッチマトリクス 10 はオフ状態とする。即ち、第 4 図の行列式の要素を全て “0” となるよう ALU 2 から指令し、全てのスリーステートバッファを OFF とする。このとき、内部バス 1 上のデータは入出力部 6 を通して出力できないので、観測することはできない。この状態で ROM 5 に格納された一連の行列データを含むプログラムにより、データテーブル 11 に

行列データを設定する。すべてのデータを設定した時点で信号線 12 を介してスイッチマトリクス 10 を構成する各スイッチをオン又はオフする。これにより内部バス 1 はバス切換回路 9、入出力部 6 を通して外部と通ずる。従ってマイクロコンピュータの内部ではプログラム、データともに暗号化されていないデータ形式の状態であるが、一旦外部へ読み出そうとするとバス切換回路 9 により暗号化された別形式の信号として出力される。また、一旦取り出したこの暗号化されたプログラム、データを外部より入力した場合、バス切換回路を通すことにより自動的に復号される。このときデータテーブル 11 の設定条件を暗号化時と同一条件としている。

本実施例の場合、ROM 5 に格納された暗号化プログラムやデータテーブル 11 内の暗号化用データもバス切換回路 9 を通して暗号化され外部のディスク 14 へ出力することができるので、読み出し不可能領域を設ける必要がなくなる。

このとき、予め ROM 5 の暗号化プログラムを

秘密保管してれば、この暗号化プログラムを使用して、取り出した暗号データや暗号プログラムを必要に応じて解読できる。

なお、上記実施例では、ROM 5 を内蔵したものを示したが、リセット時にデータテーブル 11 が一意に定まり、それに従ってスイッチマトリクス 10 がオン状態になれば、ROM 5 がなくてもよい。

また、上記実施例では、バスを構成する信号線 I₁ ~ I₈ のすべてを切換える回路について説明したが、一部の信号線 I₁ ~ I₈ のみを切換える回路であっても上記実施例と同様の効果を奏する。

なお、データテーブル 11 のデータ設定については、ALU 2 の持つ乱数発生機能を利用し、乱数により第 4 図の行列データを決定するようにしてもよい。このときは外部に取り出した暗号化プログラムは外部では解読できない。

又データテーブル 11 のデータ設定は、ALU 2 が処理する一連のデータやタスクプログラム毎に変更できるので、第 3 者が処理の内容を取り出

して知ることは殆ど不可能となる。

(発明の効果)

以上説明してきたように、この発明によれば、データやプログラムをデータ演算部の指令や記憶部内のデータに基づいて暗号化するバス切換回路をデータ演算部及び記憶部と入出力部との間に介装したので、特別に暗号化したプログラムやデータを入力する必要がなく、暗号化を行うバス切換回路の内容も外部に読み出してきた。

なお、本来の機能であるプログラムやデータの全てを暗号でき、暗号化の形式も自由に設定できる。

4. 図面の簡単な説明

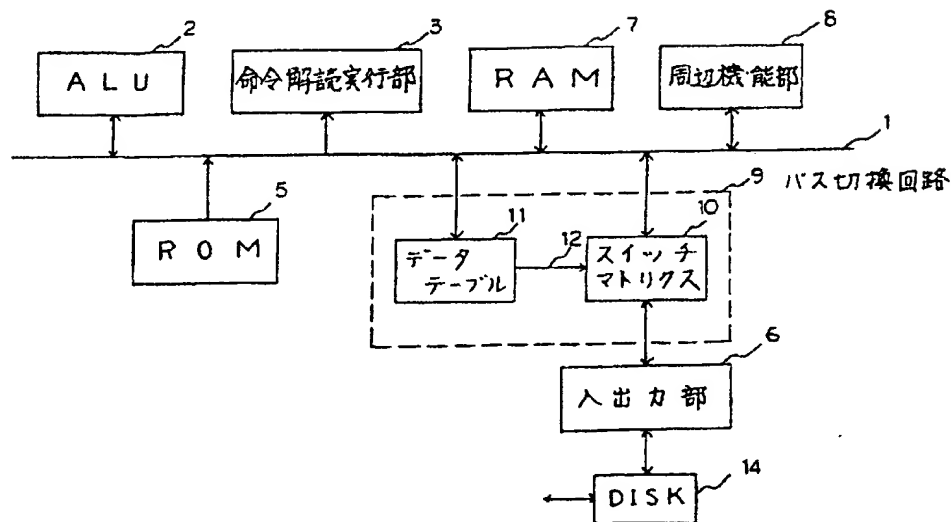
第1図はこの発明の一実施例によるマイクロコンピュータのブロック図、第2図は本発明のスイッチマトリクスの機能的構成図、第3図はスイッチマトリクスの具体的な回路の一例を示す図、第4図はデータテーブルの内容の一例を示す図、第5図は従来のマイクロコンピュータのブロック図である。

2はデータ演算部、5はROM、7はRAMの記憶部、6は入出力部、9はバス切換回路、10はスイッチマトリクス、11はデータテーブル、12は信号線である。

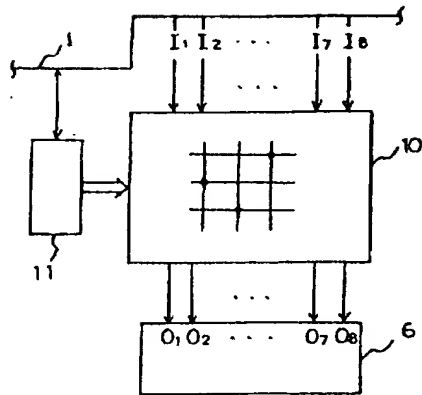
なお、図中、同一符号は同一、又は相当部分を示す。

代理人 弁理士 宮園 純一

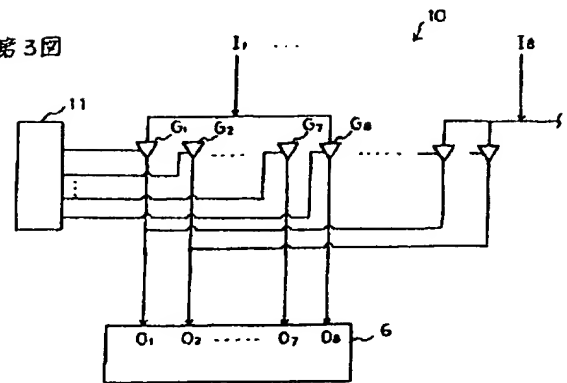
第1図



第2図



第3図

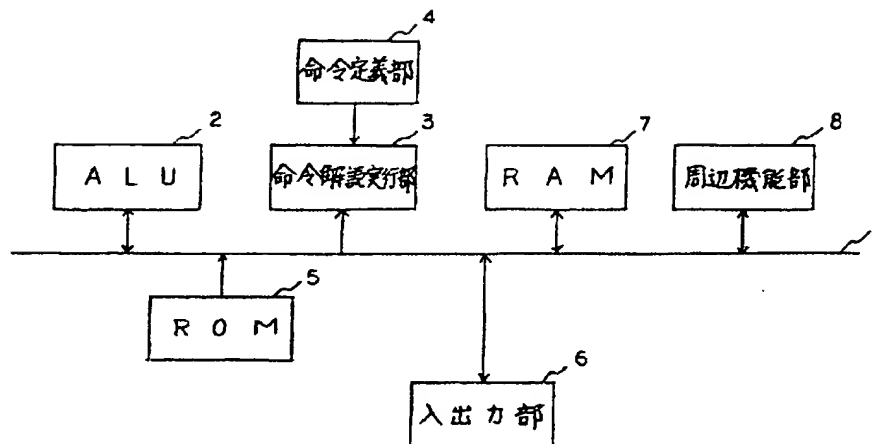


第4図

$$I_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & 1 \\ & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{matrix} O_1 \\ \leftarrow \text{行} \end{matrix}$$

↑
判

第5図



手 続 補 正 書 (自発)

平成 3 年 5 月 14 日

特許庁長官殿

1. 事件の表示 特願平2-271255号

2. 発明の名称 マイクロコンピュータ

3. 補正をする者

事件との関係 特許出願人
住 所 東京都千代田区丸の内二丁目2番3号
名 称 (601)三菱電機株式会社
代表者 志 岐 守 哉

4. 代 理 人

住 所 東京都千代田区飯田橋二丁目9番4-405
富田国際特許事務所
氏 名 (8028)弁理士 富 田 純 一
(連絡先 03(3234)5650)

5. 補正の対象

明細書の発明の詳細な説明の欄。

6. 補正の内容

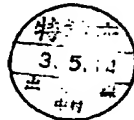
(1)明細書第2頁第4行目「復合」とあるのを「復号」と補正する。

(2)同書第2頁第10行目乃至第11行目「プログラムやデータが」とあるのを「プログラムが」と補正する。

(3)同書第3頁第1行目、第8頁第15行目「ALU2」とあるのを「命令解釈実行部3」と補正する。

(4)同書第4頁第13行目、第19行目「指令」とあるのを「データ」と補正する。

以 上



(54) CARRY LOOK-AHEAD ADDER

(11) 2-297625 (A) (43) 10.12.1990 (19) JP

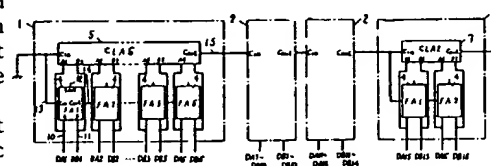
(21) Appl. No. 64-118955 (22) 12.5.1989

(71) MATSUSHITA ELECTRIC IND CO LTD (72) SHUJI NAKAYA(7)

(51) Int. Cl.³. G06F7/50

PURPOSE: To accelerate a processing by setting the number of bits to perform the arithmetic operation of a group at the most significant bit side less than that to perform the arithmetic operation of the group of a low-order bit at the most significant bit side, and adding the reduced number of bits on the bit to perform the arithmetic operation of the group at a low-order bit side.

CONSTITUTION: The number of bits to perform the arithmetic operation at the most significant bit side is set less than that to perform the arithmetic operation of the low-order bit of the group at the most significant bit side, and the reduced number of bits is added on the bits to perform the arithmetic operation of the group at the low-order side. Therefore, addition time is decided by the time of the output signal of one-bit adder circuits 4F and A4 of a third group, and time difference to be outputted between a carry signal outputted as the most significant bit and the output signals 12 of the one-bit adder circuits 4F and A4 of the third group to decide the addition time can be reduced. In such a way, it is possible to attain the acceleration of processing speed as a whole.



1: first group, 2: second group/third group, 3: fourth group

(54) SYSTEM FOR MASKING CONTENTS OF PROGRAM AND DATA

(11) 2-297626 (A) (43) 10.12.1990 (19) JP

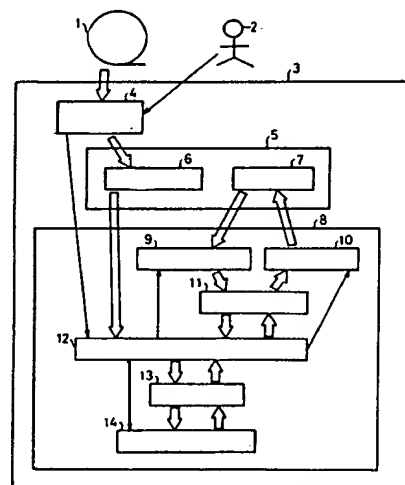
(21) Appl. No. 64-118898 (22) 12.5.1989

(71) NEC CORP (72) SHIGEYA MATSUO

(51) Int. Cl.³. G06F9/06, G06F12/14

PURPOSE: To mask the content of a program even when a memory device is referred during the execution of the program by converting the instruction of an enciphering program to a form feasible with a program execution means by an enciphering program decoding means.

CONSTITUTION: When a user starts up a program execution start means 4, the program execution start means 4, after setting an enciphering supply program 1 as the enciphering program 6, starts up the program execution means 12. The program execution means 12 takes out the instruction from the enciphering program 6 set on the memory device 5, and after setting it on an instruction decoding buffer 13, starts up the enciphering program decoding means 14. The enciphering program decoding means 14 decodes the instruction set at the instruction decoding buffer 13, and converts it to the form feasible with the program execution means 12, and sets it on the instruction decoding buffer 13. In such a way, it is possible to mask the contents of the program 1 and data 7.



3: user system, 8: central processing unit, 9: enciphering data decoding means, 10: data enciphering means, 11: data buffer

(54) SYSTEM FOR TRANSFER OF IMMEDIATE DATA AND EXECUTION OF ARITHMETIC INSTRUCTION

(11) 2-297627 (A) (43) 10.12.1990 (19) JP

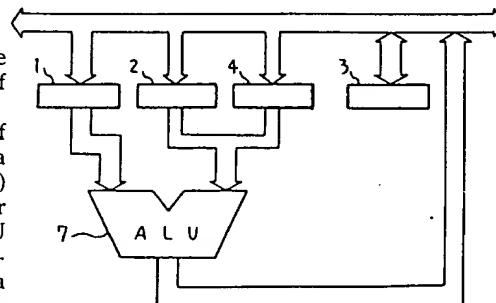
(21) Appl. No. 64-119304 (22) 11.5.1989

(71) NEC CORP (72) YUKO NINOMIYA

(51) Int. Cl.³. G06F9/22, G06F9/305

PURPOSE: To reduce the numbers of instruction bytes in the transfer and the arithmetic operation of immediate data by setting the (m) high-order bits of the immediate data of (n) bits on a dedicated register.

CONSTITUTION: An immediate register 4 to store the (m) high-order bits of the immediate data of (n) bits ($m < n$) is provided. A register 2 stores the data of (n) bits calculated at an ALU 7 transiently, and a register 3 stores the (n-m) low-order bits of the data of (n) bits transiently, and the immediate register 4 stores the (m) high-order bits of the immediate of (n) bits. Also, the ALU 7 sets the data of (n) bits stored in the register 2 with an immediate data arithmetic instruction which designates only the (n-m) low-order bits of the data of (n) bits and a numeric value stored in the register 3 as the low-order bits, and executes an arithmetic operation with the data of (n) bits setting the numeric value stored in the immediate register 4 as the high-order bit. In such a way, the numbers of instruction bytes in the transfer and the arithmetic instruction can be reduced.



1: register

Best Available Copy

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

平2-297626

⑬ Int.Cl.⁵

G 06 F 9/06
12/14

識別記号

4 5 0 A
3 2 0 B

庁内整理番号

7361-5B
7737-5B

⑭ 公開 平成2年(1990)12月10日

審査請求 未請求 請求項の数 1 (全4頁)

⑮ 発明の名称 プログラム及びデータの内容隠蔽方式

⑯ 特 願 平1-118898

⑰ 出 願 平1(1989)5月12日

⑱ 発 明 者 松 尾 篤 弥 東京都港区芝5丁目33番1号 日本電気株式会社内

⑲ 出 願 人 日本電気株式会社 東京都港区芝5丁目7番1号

⑳ 代 理 人 弁理士 境 廣 巳

明 細 書

1. 発明の名称

プログラム及びデータの内容隠蔽方式

2. 特許請求の範囲

暗号化された暗号化プログラムを実行するシステムに於いて、

中央処理装置と、

該中央処理装置で実行する暗号化プログラムが設定される記憶装置と、

該記憶装置に前記中央処理装置が実行する暗号化プログラムを設定すると共に、前記中央処理装置に対して暗号化プログラムの実行を指示するプログラム実行開始手段とを含む、

前記中央処理装置は、

命令解読バッファと、

該命令解読バッファに設定された暗号化プログラムを解読し、解読結果を前記命令解読バッファに設定する暗号化プログラム解読手段と、

データバッファと、

該データバッファに設定されたデータを暗号化

して前記記憶装置に設定するデータ暗号化手段と、

前記記憶装置に設定された暗号化データを解読して解読結果を前記データバッファに設定する暗号化データ解読手段と、

前記プログラム実行開始手段からの指示にตอบสนองして前記記憶手段に設定されている暗号化プログラムの命令を前記命令解読バッファに設定した後、前記暗号化プログラム解読手段を起動し、前記暗号化プログラム解読手段によって解読され、前記命令解読バッファに設定された命令が前記記憶装置にデータを設定する命令である場合は前記データバッファにデータを設定して前記データ暗号化手段を起動させ、前記記憶手段からデータを入力する命令である場合は前記暗号化データ解読手段を起動させ、前記暗号化データ解読手段により前記データバッファに設定されたデータを入力するプログラム実行手段とを含むことを特徴とするプログラム及びデータの内容隠蔽方式。

3. 発明の詳細な説明

(産業上の利用分野)

本発明はプログラム及びプログラムの実行中に記憶装置に設定するデータの内容を隠蔽することができるプログラム及びデータの内容隠蔽方式に関する。

(従来の技術)

従来より、プログラムの内容を隠蔽するため、プログラムライブラリ等に格納しておくプログラムを暗号化しておくということが行なわれているが、暗号化されたプログラムを実行する場合、従来は暗号化されたプログラムを解読した後、利用者システムの記憶装置にロードするようにしている。また、プログラムの実行中にデータを記憶装置に設定することが必要になった場合は、データをそのまま記憶装置に設定するようにしている。

(発明が解決しようとする課題)

従来は上述したように、プログラムを実行する際、暗号化されたプログラムを解読した後、記憶装置にロードするようにしており、また、プログラムの実行中にデータを記憶装置に設定することが必要になった場合、データをそのまま記憶装置

に設定するようにしているため、プログラムの実行中に記憶装置が参照された場合、プログラム及びデータの内容を隠蔽することができないという問題があった。

本発明の目的はプログラムの実行時に記憶装置が参照されても、プログラム及びデータの内容を隠蔽できるようにすることにある。

(課題を解決するための手段)

本発明は上記目的を達成するため、

暗号化された暗号化プログラムを実行するシステムに於いて、

中央処理装置と、

該中央処理装置で実行する暗号化プログラムが設定される記憶装置と、

該記憶装置に前記中央処理装置が実行する暗号化プログラムを設定すると共に、前記中央処理装置に対して暗号化プログラムの実行を指示するプログラム実行開始手段とを含み、

前記中央処理装置は、

命令解読バッファと、

該命令解読バッファに設定された暗号化プログラムを解読し、解読結果を前記命令解読バッファに設定する暗号化プログラム解読手段と、

データバッファと、

該データバッファに設定されたデータを暗号化して前記記憶装置に設定するデータ暗号化手段と、前記記憶装置に設定された暗号化データを解読して解読結果を前記データバッファに設定する暗号化データ解読手段と、

前記プログラム実行開始手段からの指示にตอบสนองして前記記憶手段に設定されている暗号化プログラムの命令を前記命令解読バッファに設定した後、前記暗号化プログラム解読手段を起動し、前記暗号化プログラム解読手段によって解読され、前記命令解読バッファに設定された命令が前記記憶装置にデータを設定する命令である場合は前記データバッファにデータを設定して前記データ暗号化手段を起動させ、前記記憶手段からデータを入力する命令である場合は前記暗号化データ解読手段を起動させ、前記暗号化データ解読手段により前

記データバッファに設定されたデータを入力するプログラム実行手段とを含んでいる。

(作 用)

プログラム実行開始手段は中央処理装置に暗号化プログラムを実行させる場合、暗号化プログラムを記憶装置に設定すると共に、中央処理装置に設けられているプログラム実行手段にプログラムの実行開始を指示する。プログラム実行手段はこの指示にตอบสนองして記憶装置に設定されている暗号化プログラムの命令をデータバッファに設定し、その後、暗号化プログラム解読手段を起動させる。暗号化プログラム解読手段は起動がかけられると、命令解読バッファに設定されている暗号化プログラムの命令を解読して命令解読バッファに設定し、プログラム実行手段は暗号化プログラム解読手段によって解読され、命令解読バッファに設定された命令を実行する。命令解読バッファに設定された命令が記憶装置にデータを設定する命令である場合には、プログラム実行手段はデータバッファにデータを設定した後、データ暗号化手段を起動

する。データ暗号化手段は起動されることにより、プログラム実行手段がデータバッファに設定したデータを暗号化して記憶装置に設定する。また、命令解読バッファに設定された命令が記憶装置に設定されているデータを入力する命令である場合にはプログラム実行手段は暗号化データ解読手段を起動する。暗号化データ解読手段は起動されることにより記憶装置に設定されているデータを入力し、解読してデータバッファに設定する。プログラム実行手段は暗号化データ解読手段がデータバッファに設定した解読済みのデータを入力する。
(実施例)

次に本発明の実施例について図面を参照して詳細に説明する。

第1図は本発明の実施例のブロック図であり、内容が暗号化された暗号化供給プログラム1を実行する利用者システム(情報処理装置)3はプログラム実行開始手段4と、記憶装置5と、中央処理装置8とから構成されており、中央処理装置8は暗号化データ解読手段9と、データ暗号化手段

その命令を実行する。その際、実行する命令が記憶装置5にデータを設定するものである場合はデータバッファ11にデータを設定した後、データの設定位置を指定してデータ暗号化手段10を起動する。これにより、データ暗号化手段10はデータバッファ11に設定されたデータを暗号化し、暗号化した内容を記憶装置5の指定された位置に暗号化データ7として設定する。また、実行する命令が記憶装置5からデータを入力するものである場合は、データの設定位置を指定して暗号化データ解読手段9を起動する。暗号化データ解読手段9は起動がかけられることにより、記憶装置5の指定された位置から暗号化データ7を入力し、入力した内容を解読して解読結果をデータバッファ11に設定する。プログラム実行手段12はデータバッファ11に解読済みのデータが設定されることにより、そのデータを入力する。

(発明の効果)

以上説明したように、本発明は、記憶装置には暗号化プログラムをそのまま設定し、プログラム

10と、データバッファ11と、プログラム実行手段12と、命令解読バッファ13と、暗号化プログラム解読手段14とを含んでいる。

次に本実施例の動作を説明する。

暗号化供給プログラム1を利用者システム3で実行する場合、利用者2はプログラム実行開始手段4を起動する。プログラム実行開始手段4は起動がかけられることにより、暗号化供給プログラム1を記憶装置5上に暗号化プログラム6として設定し、その後プログラム実行手段12を起動する。プログラム実行手段12は記憶装置5上に設定されている暗号化プログラム6から命令を取り出して命令解読バッファ13に設定した後、暗号化プログラム解読手段14を起動する。暗号化プログラム解読手段14は起動がかけられることにより、命令解読バッファ13に設定されている命令を解読してプログラム実行手段12で実行可能な形に変換し、命令解読バッファ13に設定する。

プログラム実行手段12は命令解読バッファ13に実行可能な形に変換された命令が設定されると、

実行手段により暗号化プログラムの命令を実行する場合には暗号化プログラム解読手段によって暗号化プログラムの命令をプログラム実行手段で実行可能な形に変換するようにしたものであるので、プログラムの実行中に記憶装置が参照されても、プログラムの内容を隠蔽することができる効果がある。また、更に、本発明はプログラムの実行中に記憶装置にデータを設定することが必要な場合、データ暗号化手段を用いてデータを暗号化した後に記憶装置に設定するようにしたものであるので、プログラムの実行中に記憶装置が参照されても、データの内容を隠蔽することができる効果がある。

4.図面の簡単な説明

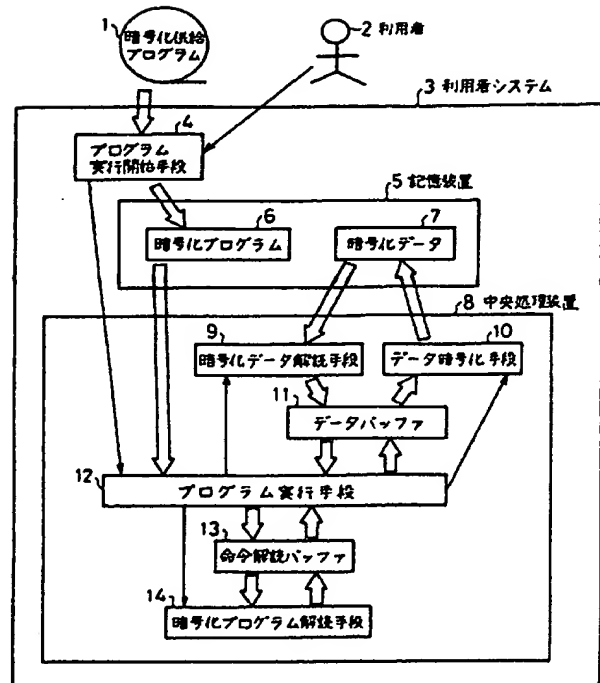
第1図は本発明の実施例のブロック図である。

図に於いて、

- 1…暗号化供給プログラム
- 2…利用者
- 3…利用者システム
- 4…プログラム実行開始手段
- 5…記憶装置

- 6…暗号化プログラム
- 7…暗号化データ
- 8…中央処理装置
- 9…暗号化データ解読手段
- 10…データ暗号化手段
- 11…データバッファ
- 12…プログラム実行手段
- 13…命令解読バッファ
- 14…暗号化プログラム解読手段

特許出願人 日本電気株式会社
代理人 弁理士 境 廣 巳



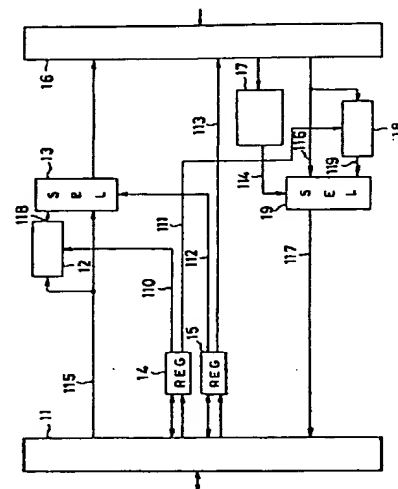
本発明の実施例のブロック図
第1図

(54) DISK CONTROLLER

(11) 5-314014 (A) (43) 26.11.1993 (19) JP
 (21) Appl. No. 4-114864 (22) 7.5.1992
 (71) TOSHIBA CORP (72) KAZUYOSHI KUWABARA
 (51) Int. Cl.⁵ G06F12/14, G06F3/06, G06F9/06

PURPOSE: To incorporate hardware for enciphering and deciphering data into a disk controller.

CONSTITUTION: The data to show whether the data generated by an external device is to be enciphered and written or not is set in a register 14, and an encipherment key is set in the register 15, and at the time of writing the data to a disk device, by referring to contents set in each register 14, 15, raw write data or write data having passed through an encipherment circuit 12 is outputted to a disk control apt 16 together with attribute information to show whether it is enciphered or not, and at the time of read, whether read data is enciphered or not is judged by judgement logic 17, and raw read data or the read data having passed through a decipherment circuit 18 is outputted to the external device in conformity with this judged result.



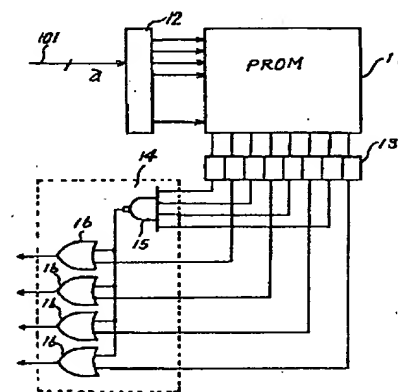
11: bus interface circuit

(54) MICROCOMPUTER

(11) 5-314015 (A) (43) 26.11.1993 (19) JP
 (21) Appl. No. 4-86782 (22) 8.4.1992
 (71) NEC CORP (72) HISAO ISHIZUKA
 (51) Int. Cl.⁵ G06F12/14, G06F15/78

PURPOSE: To prevent the PROM incorporated microcomputer from being read by an outsider in the microcomputer provided with the built-in PROM.

CONSTITUTION: This microcomputer is constituted so as to be provided with the PROM 11, an address decoder 12, a data storage circuit 13 to store the data of 8-bits read out of the PROM 11, a NAND circuit 15, and a protection circuit 14 including four OR circuits 16. Besides, original data length is made 4-bits, and the overhead bits of 4-bits are given to it. The original data and the overhead bits are arranged alternately, and total 8-bits are read out in accordance with one address. In the case that one bit among the overhead bits of 4-bits is logical "0", the protection circuit 14 outputs logical "1" all for the data of that address. Since the normal bits and the overhead bits are placed alternately, it is very difficult to erase only the overhead bits by the irradiation of ultraviolet ray, etc. Accordingly, it becomes impossible to read out a program.



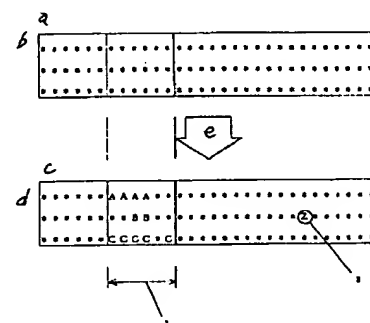
a: 8-bits

(54) AREA DESTRUCTION DETECTING SYSTEM

(11) 5-314016 (A) (43) 26.11.1993 (19) JP
 (21) Appl. No. 4-113349 (22) 6.5.1992
 (71) HITACHI LTD (72) SHUICHI ISHII(1)
 (51) Int. Cl.⁵ G06F12/16, G06F9/46, G06F15/00

PURPOSE: To always detect destruction in the case that an area assigned to another task is destroyed irrespective of whether it bestrides the boundary of the area or not by filling up a whole area pool for the task with a specified character.

CONSTITUTION: As for the area pools prepared in the number of the tasks, the whole area is filled up with the specified character at the time of starting the task, and the whole area pool is checked on the occasion of an area release request and module link, etc., and when the destruction of the specified character in the area other than that assigned to that task is detected, a warning is issued. In the area pool (i) corresponding to the task (i), the whole area is filled up with the specified character (*) at the time of starting the task (i), and the whole area pool (i) is checked on the occasion of the area release request and the module link, etc. In this case since (*) is painted out by another character (in this case, Z) in the area other than that assigned to the task (i), it is considered to be the destruction of the area assigned to another task, and the warning is issued.



a: time of start, b: area pool (i), c: time of release, d: area pool (i), e: processing

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平5-314014

(43)公開日 平成 5 年(1993)11月26日

(51)Int.Cl.⁵

G 0 6 F 12/14
3/06
9/06

識別記号

3 2 0 B 9293-5B
3 0 4 H 7165-5B
4 5 0 A 7232-5B

庁内整理番号

F I

技術表示箇所

審査請求 未請求 請求項の数 2 (全 5 頁)

(21)出願番号 特願平4-114864

(22)出願日 平成 4 年(1992) 5 月 7 日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 桑原 和義

東京都青梅市末広町 2 丁目 9 番地 株式会
社東芝青梅工場内

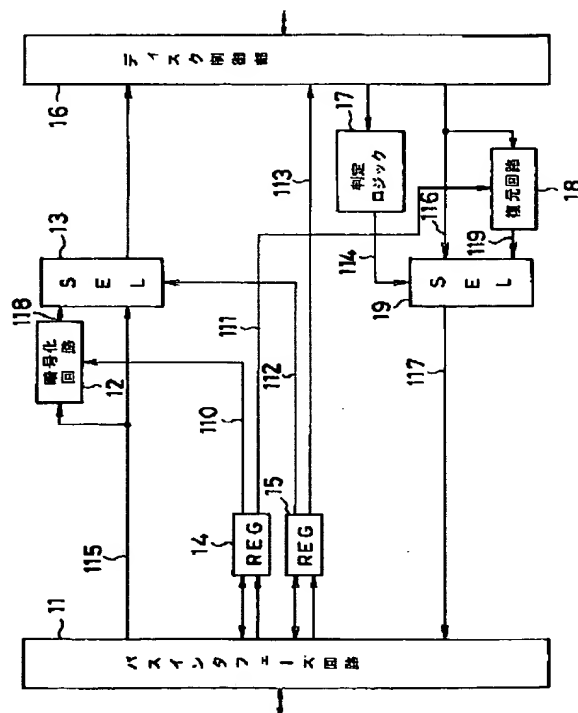
(74)代理人 弁理士 鈴江 武彦

(54)【発明の名称】 ディスクコントローラ

(57)【要約】

【目的】本発明は、データ暗号化、復元のためのハードウェアをディスクコントローラに内蔵させたことを主な特徴とする。

【構成】外部装置が生成するデータを暗号化して書き込むか否かのデータをレジスタ 1 4 に設定し、暗号化キーをレジスタ 1 5 に設定して、ディスク装置にデータを書き込む際、それぞれのレジスタ 1 4、1 5 に設定された内容を参照することにより、生の書き込みデータ又は暗号化回路 1 2 を経由した書き込みデータを、暗号化したか否かの属性情報とともにディスク制御部 1 6 へ出力し、読込みの際に、読込みデータが暗号化されているか否かを判定ロジック 1 7 によって判断し、その判断結果に従い、生の読込みデータ又は復元回路 1 8 を経由した読込みデータを外部装置に送出することを特徴とする。



【特許請求の範囲】

【請求項1】 書き込みデータの暗号化指示情報を貯える第1のレジスタ、及び暗号化のためのキー情報を貯える第2のレジスタと、

上記第1のレジスタが暗号化指示状態にあるとき、上記第2のレジスタに貯えられたキー情報を用いて外部より供給された書き込みデータを暗号化処理し、暗号化データであることを示す属性情報を付加してディスクに書き込む手段と、

上記ディスクより読込まれたデータの属性情報をもとに読込みデータが暗号化されているか否かを判断し、読込みデータが暗号化されているとき、上記第2のレジスタに貯えられたキー情報を用いて読込みデータを復号化処理する手段とを具備してなることを特徴とするディスクコントローラ。

【請求項2】 外部より設定される暗号化のためのキー情報を貯える暗号化キーレジスタと、

外部より供給される書き込みデータを暗号化するか否かを示す指示情報を貯えるデータ暗号化レジスタと、

上記暗号化キーレジスタに貯えられたキー情報をもとに外部より供給される書き込みデータに演算を施し書き込みデータを暗号化するデータ暗号化回路と、

上記データ暗号化レジスタが示す指示情報に従い、上記データ暗号化回路を経て出力されるデータ又は外部より供給される生データのいずれか一方を選択し出力する第1のデータセクタと、

この第1のデータセクタを介して出力されるデータに、上記データ暗号化レジスタの内容に従う、書き込みデータが暗号化されているか否かを示す属性情報を付加してディスク上の指定された領域に書き込むデータ書き込み手段と、

上記ディスク上の指定された領域よりデータとそのデータに付随する属性情報を読み込むデータ読込み手段と、上記ディスク上より読込まれた暗号化データを上記暗号化キーレジスタに貯えられたキー情報をもとに復元する復元回路と、

上記ディスク上より読込まれたデータの属性情報をもとに読込みデータが暗号化されているか否かを判定する判定ロジックと、

この判定ロジックの判定結果に従い、上記ディスク上より読込まれた生データ又は上記復元回路を経た読込みデータのいずれか一方を選択し外部へ出力する第2のデータセクタとを具備してなることを特徴とするディスクコントローラ。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 この発明は、特にディスク記憶装置を本体より脱着可能としたパーソナルコンピュータに用いて好適なセキュリティ機能を内蔵したディスクコントローラに関する。

【0002】

【従来の技術】 近年、オフィスでの事務の合理化が進み、その一環として、各自が1台のパーソナルコンピュータをローエンドマシンとして持ち、この各パーソナルコンピュータをLAN回線で共通に接続して、ファイルの共有化を図ったシステムが構築されている。この際、用いられるパーソナルコンピュータは、性能の向上が目覚ましく、デスクトップタイプから、小型、軽量で、携帯に便利な、所謂ラップトップタイプがその主流を占めるようになった。性能的にはデスクトップと何等の遜色もなく、最近では比較的大容量の磁気ディスク装置を補助記憶として標準装備されたものも出現してきている。

【0003】 この種OA（オフィスオートメーション）分野に於いて用いられるパーソナルコンピュータは、現状ではセキュリティ管理がハードウェアもしくはOS（オペレーティングシステム）にて殆どなされていない。その理由は、セキュリティ機能をOSで実現すると、既存OSとの互換性がなくなり、市場に流通している豊富なソフトウェア資産が利用できなくなるという問題が生じることにある。

【0004】

【発明が解決しようとする課題】 上述したように従来のOA分野で使用されるパーソナルコンピュータに於いては、セキュリティ機能をOSで実現すると、既存OSとの互換性がなくなり、市場に流通している豊富なソフトウェア資産が利用できなくなるという問題が生じる。この種パーソナルコンピュータの分野に於いて既存OSとの互換性を維持することが最重要設計事項とされることは周知の通りである。

【0005】 この発明は上記事情に鑑みてなされたもので、データ暗号化／復号化機能をディスクコントローラに持たせることにより、システム本体のCPUに処理負担をかけることなくセキュリティ管理機能を強化したパーソナルコンピュータシステムが容易に構築できるディスクコントローラを提供することを目的とする。

【0006】

【課題を解決するための手段】 本発明のディスクコントローラは、図1に示すように、ディスクへ書き込む書き込みデータを暗号化するか否かの情報を貯えるデータ暗号化レジスタ15と、暗号化のためのキー情報が外部より設定される暗号化キーレジスタ14と、暗号化キーレジスタ14に設定されたキー情報に従い外部装置から供給される書き込みデータに演算を施し暗号化するデータ暗号化回路12と、データ暗号化レジスタ15が示す値に従い、暗号化回路12を経て出力される暗号化された書き込みデータ又は外部装置から供給される生の書き込みデータのいずれか一方を選択する第1のデータセクタ（書き込みデータセクタ）13と、この第1のデータセクタ13で選択されたデータとともに当該データが暗号化さ

れているか否かの属性情報をディスク制御部16へ供給する信号線113と、磁気ディスク装置から読込まれたデータに付随する属性情報に従い当該読込みデータが暗号化されているか否かを判断する判定ロジック17と、磁気ディスク装置より読込まれた暗号化されたデータを上記暗号化キーレジスタ14のキー情報に従い復号化する復元回路18と、磁気ディスク装置より読込まれた生の読込みデータ又は上記復元回路18を経た読込みデータを受けて、上記判定ロジック17の判定結果に従い、いずれか一方のデータを選択する第2のデータセクタ（読込みデータセクタ）19とを具備することを特徴とする。

【0007】

【作用】本発明は、書き込みデータの暗号化処理を選択的に行なうハードウェアと、読込みデータの復元（復号）処理を選択的に行なうハードウェアとをディスクコントローラに持たせて、書き込みデータを任意に暗号化処理してディスクに格納し、復元（復号）処理して外部装置に渡すことができる構成としたもので、これにより、上位の外部装置（例えばパーソナルコンピュータ本体）に処理負担をかけることなく、セキュリティ管理機能の強化が図れる。

【0008】即ち本発明は、ディスクコントローラに、ディスクへ書き込む書き込みデータを暗号化するか否かの情報を貯えるデータ暗号化レジスタと、暗号化のためのキー情報が外部より設定される暗号化キーレジスタとを設け、この各レジスタに、パーソナルコンピュータ本体等の外部装置が生成するデータを暗号化して書き込むか否かのデータと、暗号化のためのキーを設定する。外部より与えられた書き込みデータをディスク装置に書き込む際に、上記各レジスタに設定された内容を参照して、外部より与えられた生の書き込みデータ又は暗号化回路を経たデータをディスク制御部へ出力し、同時に当該データが暗号化されているか否かの情報を属性情報としてディスク制御部へ出力する。ディスク制御部はこの書き込みデータ及び属性情報を磁気ディスクに記録する。ディスク制御部の制御でディスク装置よりデータが読込まれると、判定ロジックがその読込みデータに付随する属性情報から読込みデータが暗号化されているか否かを判定し、その判定結果に従うセクタのデータ選択で、生の読込みデータもしくは復元回路を経由した読込みデータが外部へ送出される。

【0009】これにより、本体CPUに処理負担をかけることなく、磁気ディスク装置の格納データを必要に応じて暗号化でき、セキュリティ管理の強化が図れる。また、暗号化、復元化がOSに依存しないため、既存OSとの互換性が維持され、現在ある豊富なソフトウェア資産を継承することができる。

【0010】

【実施例】以下、図面を使用して本発明の実施例につい

て説明する。図1は本発明の実施例を示すブロック図である。

【0011】図に於いて、符号11はバスインタフェース回路であり、この回路にて本発明の磁気ディスクコントローラと、パーソナルコンピュータ本体等の外部回路とのインタフェース接続がなされる。

【0012】符号12はデータ暗号回路であり、ライン110上の暗号化キーレジスタ14のキー情報に従い、バスインタフェース回路11、及びライン115を介して入力された外部の書き込みデータを暗号化する。

【0013】符号13は書き込みデータセクタ（SEL）であり、ライン112上のデータ暗号化レジスタ15の値により、ライン115を介して供給される生の書き込みデータ、又はライン118上のデータ暗号回路12より出力される書き込みデータのいずれか一方を選択し出力する。

【0014】符号14は暗号化キーレジスタであり、バスインタフェース回路11を介して暗号化／復号化を行なうためのキー情報（キーワード）が設定される。符号15はデータ暗号化レジスタであり、バスインタフェース回路11を介して書き込みデータを暗号化するか否かを示す値が設定される。

【0015】符号16は例えば外部接続される磁気ディスク装置を制御対象下におくディスク制御部であり、外部接続される磁気ディスク装置の機構部を制御するとともに、磁気ディスク装置との間のデータの入出力制御を行なう。ここでは

【0016】符号17はディスクの読込み対象データが暗号化されているか否か（即ち復元（復号化）処理を行なうか否か）を判定する判定ロジックであり、磁気ディスク制御部16からの読込みデータを復元すべきか否かを後述する属性情報に従い決定する。

【0017】符号18はデータ復元回路（データ復号化回路）であり、入力信号ライン116上の読込みデータ（暗号化されたデータ）をライン111上の暗号化キーレジスタ14のキー値をもとに通常の生データに復元する。

【0018】符号19は読込みデータセクタ（SEL）であり、判定ロジック17の判定結果に従い、ライン116上の生の読込みデータ、又はライン119上のデータ復元回路18を経た読込みデータのいずれか一方を選択し、データライン117上に出力する。

【0019】符号110、111は暗号化キー信号ラインであり、暗号化キーレジスタ14の内容を暗号化回路12、及び復元化回路18に伝達する。符号112、113は暗号化セレクト信号ラインであり、データ暗号化レジスタ15に設定された値を書き込みデータセクタ13、及びディスク制御部16に伝達する。符号114は復元化セレクト信号ラインであり、判定ロジック17の判定結果の情報を読込みデータセクタ19に伝達す

る。符号115は出力信号ラインであり、バスインタフェース回路11で受けた、CPU、メモリ等の外部回路からの生データを書込みデータセクタ13を介しディスク制御部16に伝達する。符号116は入力信号ラインであり、外部接続される磁気ディスクからのデータを読込みデータセクタ19に伝達する。符号117は復元済み信号ラインであり、このラインを介して読込みデータセクタ19を経たデータがバスインタフェース回路11に転送される。符号118は暗号化回路12の出力を書込みデータセクタ13を介しディスク制御部16に伝達する信号ラインであり、符号119は復元回路18の出力を読込みデータセクタ19、及び復元済み信号ライン117を介しバスインタフェース回路11に伝達する信号ラインである。以下、図1を参照して本発明の実施例の動作について説明する。まず、ディスク装置への書き込み動作を説明する。

【0020】ディスク装置への書き込みを行なう場合は、書き込みを始めるに際し、磁気ディスクコントローラの外部装置、即ち、図示しないパーソナルコンピュータ本体から、暗号化キーレジスタ14に暗号化キーが書込まれ、データ暗号化レジスタ15に暗号化するか否かの情報が書き込まれる。

【0021】データ書き込みの開始が指示されると、バスインタフェース回路11は、磁気ディスクコントローラの外部装置（パーソナルコンピュータ本体）から供給される書き込みデータを取り込み、ライン115に載せる。ライン115上の信号は、暗号化回路12と書込みデータセクタ13に供給される。

【0022】暗号化回路12は書込みデータセクタ13に設定された値に従って入力データの暗号化を行い、ライン118に載せる。書込みデータセクタ13は、データ暗号化レジスタ12の内容に従い、2つの入力ライン115、118のいずれか一方を選択し、そのライン上のデータをディスク制御部16へ出力する。このとき、データ暗号化レジスタ12の内容は、ライン113によってディスク制御部16へも渡される。

【0023】ディスク制御部16は、書込みデータセクタ13を介して出力される書込みデータに、当該書込みデータが暗号化されているか否かを示すライン113上の属性情報を付随して磁気ディスク装置に書き込む。次に、磁気ディスク装置からのデータの読み込み動作を説明する。

【0024】磁気ディスク装置に格納されたデータの読み込みを行なう場合は、読み込みを始めるに際し、外部装置（パーソナルコンピュータ本体）より、暗号化キーレジスタ14に、暗号化キーを書き込んでおく。

【0025】読み込み開始が指示されると、ディスク制*

* 御部16は、磁気ディスク装置から読み込んだデータに付随する属性情報を判定ロジック17に渡し、さらに読込みデータをライン116上に載せる。

【0026】判定ロジック17は、属性情報から、読み込みデータが暗号化データであるか非暗号化データであるかを判定し、その判定結果をライン114を介して読込みデータセクタ19に供給する。ライン116に載せられた読込みデータは、復元回路18、及び読込みデータセクタ19に供給される。

10 【0027】復元回路18は入力された読込みデータを暗号化キーレジスタ14のキー内容に従い復元（復号処理）し、その復元した読込みデータをライン119上へ出力する。

【0028】読込みデータセクタ19は、ライン114上の判定結果の指示に従い、2つの入力ライン116、119を介して得られる読込みデータのいずれか一方を選択し、ライン117上へ出力する。ライン117上の読込みデータは、バスインタフェース回路11を介して外部装置（パーソナルコンピュータ本体）に内蔵のメモリに転送される。

20 【0029】尚、上記した実施例では、ディスクコントローラに接続される外部メモリを磁気ディスク装置に限定して説明したが、これに限るものではなく、例えば光ディスク装置、光磁気ディスク装置等にも同様に応用できる。

【0030】

【発明の効果】以上説明のように本発明によれば、ディスクコントローラにデータ暗号化機能を設けた構成としたことにより、磁気ディスク装置をアクセス対象下におく本体CPUに処理負担をかけることなく、セキュリティ管理機能を強化することができる。即ち、従来、本体CPUで行なってきたセキュリティ管理のための暗号化／復号化の処理作業をハードウェア（磁気ディスクコントローラ）で行なうため、本体CPUが持つ本来の性能（処理速度）を十分に活かすことができる。更に、データの圧縮伸張、暗号化、復元化がOSに依存されずハードウェアで実現されるため、現在の豊富なソフトウェア資産を継承することができる。

【図面の簡単な説明】

40 【図1】本発明の実施例の構成を示すブロック図。

【符号の説明】

11…バスインタフェース回路、12…データ暗号化回路、13…書込みデータセクタ（SEL）、14…暗号化キーレジスタ（REG）、15…データ暗号化レジスタ（REG）、16…ディスク制御部、17…判定ロジック、18…データ復元回路（データ復号化回路）、19…読込みデータセクタ（SEL）。

【図1】

